Exhibit D Part 2

Exhibit 79

0 +0.00137 (+0.11%)







S&P 500 3710.6 +4. ◆



Sidney Powell's Legal Team Has Binder of Documents She Says Establish the 2020 Election was a Fraud



(Claire Swift/Zenger News)

Zenger News publishes the Powell binder in its entirety.

In a Dec. 23, 2020 interview with Zenger News, attorney Sidney Powell stepped through a binder of information her legal team provided two hours before cameras rolled.



Powell contends that documents in the binder prove direct foreign interference and



Access Email Faster
 easyemailsuite.com

Powell contends that documents in the binder prove direct foreign interference and fraud tainted the Nov. 3 presidential election, and that President Donald Trump was re-elected. The entire binder is reproduced here for exclusively.











© Z News Service, Inc. 2020. All Rights Reserved. 2303 Ranch Road, 620 South, Suite 160-125, Austin, Texas 78734 About Us

Press

Ethics

Corrections

Who was John Peter Zenger?

Register

Contact Us

FAQ

Privacy Policy

Terms & Conditions

Trademarks

Document title: Pals Sidney Powell #39: Ling in Inaud #39: Ling in In



The following is a faithful reproduction of a binder of documents provided to Zenger News by Sidney Powell's legal team on Dec. 23, 2020.

Zenger News has not edited it in any way and is not responsible for its contents.

Table of Contents

- CISA-FBI Alerts on Iranian Election Interference: Iranian Advanced Persistent Threat Actor Identified Obtaining Voter Registration Data (AA20-304A)
- CISA-FBI Alerts on Iranian Election Interference: Iranian Advanced Persistent Treat Actors Threaten Election-Related Systems (AA20-296B)
- 3) DHS Designation of Election Systems as Critical Infrastructure
 - a. APT Actors Chaining Vulnerabilities Against SLTT, Critical Infrastructure, Elections Organizations
- 4) Treasury Statement on Fraudulent Election Interference by Maduro Regime
- Report of the Select Committee on Intelligence United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, Volume 3: U.S. Government Response to Russian Activities
- 6) Allied Security Operations Group: Antrim Michigan Forensics Report
- Redacted Affidavit/Declaration 1
- 8) Redacted Affidavit/Declaration 2
- 9) Venezuela Statement
- Executive Order on Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election, September 12, 2018
- 11) 50 USC 1702 Presidential Authorities
- 12) Senator Warren, Klobuchar, Wyden, Pocan Letters to H.I.G.
- 13) Swiss and Aussies Find a Critical Flaw in Scyti Software that the US Ignores
- 14) The Immaculate Deception, Peter Navarro



National Cyber Awareness System > Alerts

> Iranian Advanced Persistent Threat Actor Identified Obtaining Voter Registration Data

Alert (AA20-304A)

More Alerts

Iranian Advanced Persistent Threat Actor Identified Obtaining Voter Registration Data

Original release date: October 30, 2020 | Last revised: November 03, 2020

Summary

This joint cybersecurity advisory was coauthored by the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI). CISA and the FBI are aware of an Iranian advanced persistent threat (APT) actor targeting U.S. state websites—to include election websites. CISA and the FBI assess this actor is responsible for the mass

This advisory uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) version 8 framework. See the ATT&CK for Enterprise version 8 for all referenced threat actor techniques.

dissemination of voter intimidation emails to U.S. citizens and the dissemination of U.S. election-related disinformation in mid-October 2020. ¹ (Reference FBI FLASH message ME-000138-TT, disseminated October 29, 2020). Further evaluation by CISA and the FBI has identified the targeting of U.S. state election websites was an intentional effort to influence and interfere with the 2020 U.S. presidential election.

Click here for a PDF version of this report.

Technical Details

1 of 9

Analysis by CISA and the FBI indicates this actor scanned state websites, to include state election websites, between September 20 and September 28, 2020, with the Acunetix vulnerability scanner (*Active Scanning: Vulnerability Scanning* [T1595.002]). Acunetix is a widely used and legitimate web scanner, which has been used by threat actors for nefarious

TLP:WHITE

Case 1:21-cv-00317-DCLC-CHS Document 22-7 Filed 01/20/22 Page 8 of 591 PageID #: 1566 12/22/20, 1:51 AM

This disinformation (hereinalter, "the propaganda video") was in the form of a video purporting to misattribute the activity to a U.S. domestic
actor and implies that individuals could cast fraudulent ballots, even from overseas. https://www.odni.gov/index.php/newsroom/press-releases
/itent/2162-dni-john-ratcliffe-s-remarks-at-press-conference-on-election-security.

purposes. Organizations that do not regularly use Acunetix should monitor their logs for any activity from the program that originates from IP addresses provided in this advisory and consider it malicious reconnaissance behavior.

TLP:WHITE

Additionally, CISA and the FBI observed this actor attempting to exploit websites to obtain copies of voter registration data between September 29 and October 17, 2020 (Exploit Public-Facing Application [T1190]). This includes attempted exploitation of known vulnerabilities, directory traversal, Structured Query Language (SQL) injection, web shell uploads, and leveraging unique flaws in websites.

CISA and the FBI can confirm that the actor successfully obtained voter registration data in at least one state. The access of voter registration data appeared to involve the abuse of website misconfigurations and a scripted process using the cURL tool to iterate through voter records. A review of the records that were copied and obtained reveals the information was used in the propaganda video.

CISA and FBI analysis of identified activity against state websites, including state election websites, referenced in this product cannot all be fully attributed to this Iranian APT actor. FBI analysis of the Iranian APT actor's activity has identified targeting of U.S. elections' infrastructure (Compromise Infrastructure [T1584]) within a similar timeframe, use of IP addresses and IP ranges—including numerous virtual private network (VPN) service exit nodes—which correlate to this Iran APT actor (Gather Victim Host Information [T1592)]), and other investigative information.

Reconnaissance

The FBI has information indicating this Iran-based actor attempted to access PDF documents from state voter sites using advanced open-source queries (*Search Open Websites and Domains* [T1593]). The actor demonstrated interest in PDFs hosted on URLs with the words "vote" or "voter" and "registration." The FBI identified queries of URLs for election-related sites.

The FBI also has information indicating the actor researched the following information in a suspected attempt to further their efforts to survey and exploit state election websites.

- YOURLS exploit
- · Bypassing ModSecurity Web Application Firewall
- · Detecting Web Application Firewalls
- SQLmap tool

2 of 9

Acunetix Scanning

CISA's analysis identified the scanning of multiple entities by the Acunetix Web Vulnerability scanning platform between September 20 and September 28, 2020 (Active Scanning: Vulnerability Scanning [T1595.002]).

The actor used the scanner to attempt SQL injection into various fields in /registration /registration/details with status codes 404 or 500.

/registration/registration/details?addresscity=-1 or 3*2<(0+5+513-513) -- &addressstreet1=xxxxx&btnbeginregistration=begin</p> voter registration&btnnextelectionworkerinfo=next& btnnextpersonalinfo=next&btnnextresdetails=next& btnnextvoterinformation=next&btnsubmit=submit&chkageverno=on& chkageveryes=on&chkcitizenno=on&chkcitizenyes=on&chkdisabledvoter=on& chkelectionworker=on&chkresprivate=1&chkstatecancel=on&dlnumber=1& dob=xxxx/x/x&email=sample@email.tst&firstname=xxxxx&gender=radio& hdnaddresscity=&hdngender=&last4ssn=xxxxx&lastname=xxxxxinjjeuee& mailaddresscountry=sample@xxx.xxx&mailaddressline1=sample@email.tst& mailaddressline2=sample@xxx.xxx&mailaddressline3=sample@xxx.xxx& mailaddressstate=aa&mailaddresszip=sample@xxxx.xxx& mailaddresszipex=sample@xxx.xxx&middlename=xxxxx&overseas=1& partycode=a&phoneno1=xxx-xxx-xxxx&phoneno2=xxx-xxxx&radio=consent& statecancelcity=xxxxxxx&statecancelcountry=usa&statecancelstate=XXaa& statecancelzip=xxxxx&statecancelzipext=xxxxx&suffixname=esq& txtmailaddresscity=sample@xxx.xxx

TLP:WHITE

Requests

The actor used the following requests associated with this scanning activity.

2020-09-26 13:12:56 x.x.x.x GET /x/x v[\$acunetix]=1 443 - x.x.x.x Mozilla/5.0+(Windows+NT+6.1;+WOW64)+AppleWebKit/537.21+ (KHTML,+like+Gecko)+Chrome/41.0.2228.0+Safari/537.21 - 200 0 0 0

2020-09-26 13:13:19 X.X.x.x GET /x/x voterid[\$acunetix]=1 443 - x.x.x.x Mozilla/5.0+(Windows+NT+6.1;+WOW64)+AppleWebKit/537.21+ (KHTML,+like+Gecko)+Chrome/41.0.2228.0+Safari/537.21 - 200 0 0 1375

2020-09-26 13:13:18 .X.x.x GET /x/x voterid=; print(md5(acunetix_wvs_security_test)); 443 - X.X.x.x

User Agents Observed

CISA and FBI have observed the following user agents associated with this scanning activity.

Mozilla/5.0+(Windows+NT+6.1;+WOW64)+AppleWebKit/537.21+ (KHTML,+like+Gecko)+Chrome/41.0.2228.0+Safari/537.21 - 500 0 0

Mozilla/5.0+(X11;+U;+Linux+x86_64;+en-US;+rv:1.9b4)+Gecko/2008031318+Firefox/3.0b4

Mozilla/5.0+(X11;+U;+Linux+i686;+en-US;+rv:1.8.1.17)+Gecko/20080922+Ubuntu/7.10+(gutsy)+Firefox/2.0.0.17

Exfiltration

3 of 9

Obtaining Voter Registration Data

Following the review of web server access logs, CISA analysts, in coordination with the FBI, found instances of the cURL and FDM User Agents sending GET requests to a web resource associated with voter registration data. The activity occurred between September 29 and October 17, 2020. Suspected scripted activity submitted several hundred thousand queries iterating through voter identification values, and retrieving results with varying levels of success [Gather Victim Identity Information (T1589)]. A sample of the records identified by the FBI reveals they match information in the aforementioned propaganda video. Requests

The actor used the following requests.

2020-10-17 13:07:51 x.x.x.x GET /x/x voterid=XXXX1 443 - x.x.x.x curl/7.55.1 - 200 0 0 1406

2020-10-17 13:07:55 x.x.x.x GET /x/x voterid=XXXX2 443 - x.x.x.x curl/7.55.1 - 200 0 0 1390

2020-10-17 13:07:58 x.x.x.x GET /x/x voterid=XXXXX3 443 - x.x.x.x curl/7.55.1 - 200 0 0 1625

2020-10-17 13:08:00 x.x.x.x GET /x/x voterid=XXXX4 443 - x.x.x.x curl/7.55.1 - 200 0 0 1390

Note: incrementing voterid values in cs_uri_query field

User Agents

CISA and FBI have observed the following user agents.

FDM+3.x

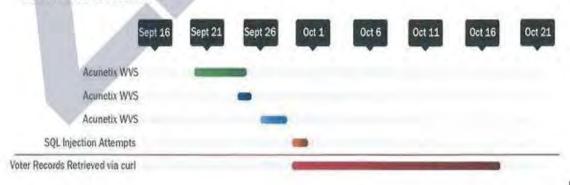
4 of 9

curl/7.55.1

Mozilla/5.0+(Windows+NT+6.1;+WOW64)+AppleWebKit/537.21+
(KHTML,+like+Gecko)+Chrome/41.0.2228.0+Safari/537.21 - 500 0 0 0 Mozilla/5.0+(X11;+U;+Linux+x86_64;+en-US;+rv:1.9b4)+Gecko/2008031318+Firefox/3.0b4

See figure 1 below for a timeline of the actor's malicious activity.

TECHNICAL FINDINGS



TLP:WHITE

Mitigations

Detection

Acunetix Scanning

Organizations can identify Acunetix scanning activity by using the following keywords while performing log analysis.

- \$acunetix
- acunetix_wvs_security_test

Indicators of Compromise

For a downloadable copy of IOCs, see AA20-304A.stix.

Disclaimer: many of the IP addresses included below likely correspond to publicly available VPN services, which can be used by individuals all over the world. This creates the potential for a significant number of false positives; only activity listed in this advisory warrants further investigation. The actor likely uses various IP addresses and VPN services.

The following IPs have been associated with this activity.

- 102.129.239[.]185 (Acunetix Scanning)
- 143.244.38[.]60 (Acunetix Scanning and cURL requests)
- 45.139.49[.]228 (Acunetix Scanning)
- 156.146.54[.]90 (Acunetix Scanning)
- 109.202.111[.]236 (cURL requests)
- 185.77.248[.]17 (cURL requests)
- 217.138.211[.]249 (cURL requests)
- 217.146.82[.]207 (cURL requests)
- 37.235.103[.]85 (cURL requests)
- 37.235.98[.]64 (cURL requests)
- 70.32.5[.]96 (cURL requests)
- 70.32.6[.]20 (cURL requests)
- 70.32.6[.]8 (cURL requests)
- 70.32.6[.]97 (cURL requests)
- 70.32.6[.]98 (cURL requests)
- 77.243.191[.]21 (cURL requests and FDM+3.x [Free Download Manager v3] enumeration/iteration)
- 92.223.89[.]73 (cURL requests)

5 of 9

CISA and the FBI are aware the following IOCs have been used by this Iran-based actor. These IP addresses facilitated the mass dissemination of voter intimidation email messages on October 20, 2020.

195.181.170[.]244 (Observed September 30 and October 20, 2020)

- 102.129.239[.]185 (Observed September 30, 2020)
- 104.206.13[.]27 (Observed September 30, 2020)
- 154.16.93[.]125 (Observed September 30, 2020)
- 185.191.207[.]169 (Observed September 30, 2020)
- 185.191.207[.]52 (Observed September 30, 2020)
- 194.127.172[.]98 (Observed September 30, 2020)
- 194.35.233[.]83 (Observed September 30, 2020)
- 198.147.23[.]147 (Observed September 30, 2020)
- 198.16.66[.]139(Observed September 30, 2020)
- 212.102.45[.]3 (Observed September 30, 2020)
- 212.102.45[.]58 (Observed September 30, 2020)
- 31.168.98[.]73 (Observed September 30, 2020)
- 37.120.204[.]156 (Observed September 30, 2020)
- 5.160.253[.]50 (Observed September 30, 2020)
- 5.253.204[.]74 (Observed September 30, 2020)
- 64.44.81[.]68 (Observed September 30, 2020)
- 84.17.45[.]218 (Observed September 30, 2020)
- 89.187.182[.]106 (Observed September 30, 2020)
- 89.187.182[.]111 (Observed September 30, 2020)
- 89.34.98[.]114 (Observed September 30, 2020)
- 89.44.201[.]211 (Observed September 30, 2020)

Recommendations

The following list provides recommended self-protection mitigation strategies against cyber techniques used by advanced persistent threat actors:

- Validate input as a method of sanitizing untrusted input submitted by web application
 users. Validating input can significantly reduce the probability of successful exploitation
 by providing protection against security flaws in web applications. The types of attacks
 possibly prevented include SQL injection, Cross Site Scripting (XSS), and command
 injection.
- Audit your network for systems using Remote Desktop Protocol (RDP) and other internet-facing services. Disable unnecessary services and install available patches for the services in use. Users may need to work with their technology vendors to confirm that patches will not affect system processes.
- Verify all cloud-based virtual machine instances with a public IP, and avoid using open RDP ports, unless there is a valid need. Place any system with an open RDP port behind a firewall and require users to use a VPN to access it through the firewall.
- Enable strong password requirements and account lockout policies to defend against brute-force attacks.
- · Apply multi-factor authentication, when possible.
- Maintain a good information back-up strategy by routinely backing up all critical data and system configuration information on a separate device. Store the backups offline, verify their integrity, and verify the restoration process.

TLP:WHITE

- Enable logging and ensure logging mechanisms capture RDP logins. Keep logs for a minimum of 90 days and review them regularly to detect intrusion attempts.
- When creating cloud-based virtual machines, adhere to the cloud provider's best practices for remote access.
- Ensure third parties that require RDP access follow internal remote access policies.
- Minimize network exposure for all control system devices. Where possible, critical devices should not have RDP enabled.
- Regulate and limit external to internal RDP connections. When external access to
 internal resources is required, use secure methods, such as a VPNs. However, recognize
 the security of VPNs matches the security of the connected devices.
- Use security features provided by social media platforms; use strong passwords, change passwords frequently, and use a different password for each social media account.
- See CISA's Tip on Best Practices for Securing Election Systems for more information.

General Mitigations

Keep applications and systems updated and patched

Apply all available software updates and patches and automate this process to the greatest extent possible (e.g., by using an update service provided directly from the vendor). Automating updates and patches is critical because of the speed of threat actors to create new exploits following the release of a patch. These "N-day" exploits can be as damaging as zero-day exploits. Ensure the authenticity and integrity of vendor updates by using signed updates delivered over protected links. Without the rapid and thorough application of patches, threat actors can operate inside a defender's patch cycle. ² Additionally, use tools (e.g., the OWASP Dependency-Check Project tool ³) to identify the publicly known vulnerabilities in third-party libraries depended upon by the application.

Scan web applications for SQL injection and other common web vulnerabilities

Implement a plan to scan public-facing web servers for common web vulnerabilities (e.g., SQL injection, cross-site scripting) by using a commercial web application vulnerability scanner in combination with a source code scanner. ⁴ Fixing or patching vulnerabilities after they are identified is especially crucial for networks hosting older web applications. As sites get older, more vulnerabilities are discovered and exposed.

Deploy a web application firewall

7 of 9

Deploy a web application firewall (WAF) to prevent invalid input attacks and other attacks destined for the web application. WAFs are intrusion/detection/prevention devices that inspect each web request made to and from the web application to determine if the request is malicious. Some WAFs install on the host system and others are dedicated devices that sit in front of the web application. WAFs also weaken the effectiveness of automated web vulnerability scanning tools.

Deploy techniques to protect against web shells

Patch web application vulnerabilities or fix configuration weaknesses that allow web shell attacks, and follow guidance on detecting and preventing web shell malware. ⁵ Malicious

TLP:WHITE

cyber actors often deploy web shells—software that can enable remote administration—on a victim's web server. Malicious cyber actors can use web shells to execute arbitrary system commands commonly sent over HTTP or HTTPS. Attackers often create web shells by adding or modifying a file in an existing web application. Web shells provide attackers with persistent access to a compromised network using communications channels disguised to blend in with legitimate traffic. Web shell malware is a long-standing, pervasive threat that continues to evade many security tools.

TLP:WHITE

Use multi-factor authentication for administrator accounts

Prioritize protection for accounts with elevated privileges, remote access, or used on high-value assets. ⁶ Use physical token-based authentication systems to supplement knowledge-based factors such as passwords and personal identification numbers (PINs). ⁷ Organizations should migrate away from single-factor authentication, such as password-based systems, which are subject to poor user choices and more susceptible to credential theft, forgery, and password reuse across multiple systems.

Remediate critical web application security risks

First, identify and remediate critical web application security risks. Next, move on to other less critical vulnerabilities. Follow available guidance on securing web applications. ^{8 9 10}

How do I respond to unauthorized access to electionrelated systems?

Implement your security incident response and business continuity plan

It may take time for your organization's IT professionals to isolate and remove threats to your systems and restore normal operations. In the meantime, take steps to maintain your organization's essential functions according to your business continuity plan. Organizations should maintain and regularly test backup plans, disaster recovery plans, and business continuity procedures.

Contact CISA or law enforcement immediately

To report an intrusion and to request incident response resources or technical assistance, contact CISA (Central@cisa.gov or 888-282-0870) or the FBI through a local field office or the FBI's Cyber Division (CyWatch@ic.fbi.gov or 855-292-3937).

Resources

- CISA Tip: Best Practices for Securing Election Systems
- CISA Tip: Securing Voter Registration Data
- CISA Tip: Website Security
- CISA Tip: Avoiding Social Engineering and Phishing Attacks
- CISA Tip: Securing Network Infrastructure Devices
- Joint Advisory: Technical Approaches to Uncovering and Remediating Malicious Activity

- CISA Insights: Actions to Counter Email-Based Attacks on Election-related Entities
- FBI and CISA Public Service Announcement (PSA): Spoofed Internet Domains and Email Accounts Pose Cyber and Disinformation Risks to Voters
- FBI and CISA PSA: Foreign Actors Likely to Use Online Journals to Spread Disinformation Regarding 2020 Elections
- FBI and CISA PSA: Distributed Denial of Service Attacks Could Hinder Access to Voting Information, Would Not Prevent Voting
- FBI and CISA PSA: False Claims of Hacked Voter Information Likely Intended to Cast Doubt on Legitimacy of U.S. Elections
- FBI and CISA PSA: Cyber Threats to Voting Processes Could Slow But Not Prevent Voting
- FBI and CISA PSA: Foreign Actors and Cybercriminals Likely to Spread Disinformation Regarding 2020 Election Result
- NSA "NSA'S Top Ten Cybersecurity Mitigation Strategies" https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/csi-nsas-top10-cybersecurity-mitigation-strategies.pdf
- https://owasp.org/www-project-dependency-check/
- 4. https://apps.nsa.gov/laarchive/library/la-guidance/tech-briefs/defending against-the-exploitation-of-sql-vulnerabilities-to.cfm
- NSA & ASD "CyberSecurity Information: Detect and Prevent Web Shell Malware" https://media.defense.gov/2020/Jun/09/2002313681/-1/-1/0/CSI-DETECT-AND-PREVENT-WEB-SHELL-MALWARE-20200422.PDF
- 6. https://us-cert.cisa.gov/cdm/event/identifying-and-Protecting-High-Value-Assets Closer-Look-Governance-Needs-HVAs
- NSA"NSA'S Top Ten Cybersecurity Mitigation Strategies" https://eww.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/csi-nsas-top10-cybersecurity-mitigation-strategies.pdf
- NSA "Building Web Applications Security for Developers" https://apps.nsa.gov/iaarchive/library/la-guidance/security tips/building-web-applications-security-recommendations-for.cfm
- https://owasp.org/www-project-top-ten/
- 10. https://cwe.mitre.org/top25/archive/2020/2020_cwe_top25.html

Revisions

9 of 9

October 30, 2020: Initial Version

November 3, 2020: Updated IOC disclaimer to emphasize that only activity listed in this alert warrants further investigation.

This product is provided subject to this Notification and this Privacy & Use policy.





Alert (AA20-296B)

More Alerts

Iranian Advanced Persistent Threat Actors Threaten Election-Related Systems

Original release date: October 22, 2020

Summary

The Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) are warning that Iranian advanced persistent threat (APT) actors are likely intent on influencing and interfering with the U.S. elections to sow discord among voters and undermine public confidence in the U.S. electoral process.

The APT actors are creating fictitious media sites and spoofing legitimate media sites to spread obtained U.S. voter-registration data, anti-American propaganda, and misinformation about voter suppression, voter fraud, and ballot fraud.

The APT actors have historically exploited critical vulnerabilities to conduct distributed denial-of-service (DDoS) attacks, structured query language (SQL) injections attacks, spearphishing campaigns, website defacements, and disinformation campaigns.

Click here for a PDF version of this report.

Technical Details

These actors have conducted a significant number of intrusions against U.S.-based networks since August 2019. The actors leveraged several Common Vulnerabilities and Exposures (CVEs)—notably CVE-2020-5902 and CVE-2017-9248—pertaining to virtual private networks (VPNs) and content management systems (CMSs).

- CVE-2020-5902 affects F5 VPNs. Remote attackers could exploit this vulnerability to execute arbitrary code. [1].
- CVE-2017-9248 affects Telerik UI. Attackers could exploit this vulnerability in web applications using Telerik UI for ASP.NET AJAX to conduct cross-site scripting (XSS) attacks.[2]

Historically, these actors have conducted DDoS attacks, SQL injections attacks, spearphishing campaigns, website defacements, and disinformation campaigns. These activities could render these systems temporarily inaccessible to the public or election officials, Case 1:21-cv-00317-DCLC-CHS Document 22-7 Filed 01/20/22 Page 17 of 591 which could slow, but would not prevent, voting or the reporting of results.

TLP:WHITE

- A DDoS attack could slow or render election-related public-facing websites inaccessible
 by flooding the internet-accessible server with requests; this would prevent users from
 accessing online resources, such as voting information or non-official voting results. In
 the past, cyber actors have falsely claimed DDoS attacks have compromised the
 integrity of voting systems in an effort to mislead the public that their attack would
 prevent a voter from casting a ballot or change votes already cast.
- A SQL injection involves a threat actor inserting malicious code into the entry field of an
 application, causing that code to execute if entries have not been sanitized. SQL
 injections are among the most dangerous and common exploits affecting websites. A
 SQL injection into a media company's CMS could enable a cyber actor access to
 network systems to manipulate content or falsify news reports prior to publication.
- Spear-phishing messages may not be easily detectible. These emails often ask victims
 to fill out forms or verify information through links embedded in the email. APT actors
 use spear phishing to gain access to information—often credentials, such as passwords
 —and to identify follow-on victims. A malicious cyber actor could use compromised
 email access to spread disinformation to the victims' contacts or collect information
 sent to or from the compromised account.
- Public-facing website defacements typically involve a cyber threat actor compromising
 the website or its associated CMS, allowing the actor to upload images to the site's
 landing page. In situations where such public-facing websites relate to elections (e.g.,
 the website of a county board of elections), defacements could cast doubt on the
 security and legitimacy of the websites' information. If cyber actors were able to
 successfully change an election-related website, the underlying data and internal
 systems would remain uncompromised..
- Disinformation campaigns involve malign actions taken by foreign governments or
 actors designed to sow discord, manipulate public discourse, or discredit the electoral
 system. Malicious actors often use social media as well as fictitious and spoofed media
 sites for these campaigns. Based on their corporate policies, social media companies
 have worked to counter these actors' use of their platforms to promote fictitious news
 stories by removing the news stories, and in many instances, closing the accounts
 related to the malicious activity. However, these adversaries will continue their
 attempts to create fictitious accounts that promote divisive storylines to sow discord,
 even after the election.

Mitigations

The following recommended mitigations list includes self-protection strategies against the cyber techniques used by the APT actors:

 Validate input—input validation is a method of sanitizing untrusted input provided by web application users. Implementing input validation can protect against security flaws of web applications by significantly reducing the probability of successful exploitation.
 Types of attacks possibly prevented include SQL injection, XSS, and command

- Audit your network for systems using Remote Desktop Protocol (RDP) and other internet-facing services. Disable the service if unneeded or install available patches. Users may need to work with their technology vendors to confirm that patches will not affect system processes.
- Verify all cloud-based virtual machine instances with a public IP; do not have open RDP. ports, unless there is a valid business reason to do so. Place any system with an open RDP port behind a firewall, and require users to use a VPN to access it through the firewall.
- Enable strong password requirements and account lockout policies to defend against brute-force attacks.
- · Apply multi-factor authentication, when possible.
- · Apply system and software updates regularly, particularly if you are deploying products affected by CVE-2020-5902 and CVE-2017-9248.
 - For patch information on CVE-2020-5902, refer to F5 Security Advisory K52145254.
 - For patch information on CVE-2017-9248, refer to Progress Telerik details for CVE-2017-9248.
- Maintain a good information back-up strategy that involves routinely backing up all critical data and system configuration information on a separate device. Store the backups offline; verify their integrity and restoration process.
- Enable logging and ensure logging mechanisms capture RDP logins. Keep logs for a minimum of 90 days, and review them regularly to detect intrusion attempts.
- When creating cloud-based virtual machines, adhere to the cloud provider's best practices for remote access.
- Ensure third parties that require RDP access are required to follow internal policies on remote access.
- · Minimize network exposure for all control system devices. Where possible, critical devices should not have RDP enabled.
- · Regulate and limit external to internal RDP connections. When external access to internal resources is required, use secure methods, such as VPNs, recognizing VPNs are only as secure as the connected devices.
- Be aware of unsolicited contact on social media from any individual you do not know.
- Be aware of attempts to pass links or files via social media from anyone you do not know.
- Be aware of unsolicited requests to share a file via online services.
- Be aware of email messages conveying suspicious alerts or other online accounts, including login notifications from foreign countries or other alerts indicating attempted unauthorized access to your accounts.
- Be suspicious of emails purporting to be from legitimate online services (e.g., the images in the email appear to be slightly pixelated and/or grainy, language in the email seems off, the email originates from an IP address not attributable to the provider/company).
- Be suspicious of unsolicited email messages that contain shortened links (e.g., via tinyurl, bit.ly).

- Use security features provided by social media platforms, use strong passwords, change passwords frequently, and use a different password for each social media account.
- See CISA's Tip on Best Practices for Securing Election Systems for more information.

General Mitigations

Keep applications and systems updated and patched

Apply all available software updates and patches; automate this process to the greatest extent possible (e.g., by using an update service provided directly from the vendor). Automating updates and patches is critical because of the speed at which threat actors create exploits after a patch is released. These "N-day" exploits can be as damaging as a zero-day exploits. Vendor updates must also be authentic; updates are typically signed and delivered over protected links to ensure the integrity of the content. Without rapid and thorough patch application, threat actors can operate inside a defender's patch cycle.[3] In addition to updating the application, use tools (e.g., the OWASP Dependency-Check Project tool[4]) to identify publicly known vulnerabilities in third-party libraries that the application depends on.

Scan web applications for SQL injection and other common web vulnerabilities

Implement a plan to scan public-facing web servers for common web vulnerabilities (SQL injection, cross-site scripting, etc.); use a commercial web application vulnerability scanner in combination with a source code scanner.[5] As vulnerabilities are found, they should be fixed or patched. This is especially crucial for networks that host older web applications; as sites get older, more vulnerabilities are discovered and exposed.

Deploy a web application firewall

Deploy a web application firewall (WAF) to help prevent invalid input attacks and other attacks destined for the web application. WAFs are intrusion/detection/prevention devices that inspect each web request made to and from the web application to determine if the request is malicious. Some WAFs install on the host system and others are dedicated devices that sit in front of the web application. WAFs also weaken the effectiveness of automated web vulnerability scanning tools.

Deploy techniques to protect against web shells

Patch web application vulnerabilities or fix configuration weaknesses that allow web shell attacks, and follow guidance on detecting and preventing web shell malware.[6] Malicious cyber actors often deploy web shells-software that can enable remote administration-on a victim's web server. Malicious cyber actors can use web shells to execute arbitrary system commands, which are commonly sent over HTTP or HTTPS. Attackers often create web shells by adding or modifying a file in an existing web application. Web shells provide attackers with persistent access to a compromised network using communications channels disguised to blend in with legitimate traffic. Web shell malware is a long-standing, pervasive threat that continues to evade many security tools.

Use multi-factor authentication for administrator accounts

Prioritize protection for accounts with elevated privileges, with remote access, and/or used on high value assets.[7] Use physical token-based authentication systems to supplement knowledge-based factors such as passwords and personal identification numbers (PINs). [8] Organizations should migrate away from single-factor authentication, such as password-based systems, which are subject to poor user choices and more susceptible to credential theft, forgery, and password reuse across multiple systems.

Remediate critical web application security risks

First, identify and remedite critical web application security risks first; then, move on to other less critical vulnerabilities. Follow available guidance on securing web applications. [9],[10],[11]

How do I respond to unauthorized access to election-related systems?

Implement your security incident response and business continuity plan

It may take time for your organization's IT professionals to isolate and remove threats to your systems and restore normal operations. In the meantime, take steps to maintain your organization's essential functions according to your business continuity plan. Organizations should maintain and regularly test backup plans, disaster recovery plans, and business continuity procedures.

Contact CISA or law enforcement immediately

To report an intrusion and to request incident response resources or technical assistance, contact CISA (Central@cisa.dhs.gov or 888-282-0870) or the Federal Bureau of Investigation (FBI) through a local field office or the FBI's Cyber Division (CyWatch@ic.fbi.gov or 855-292-3937).

Resources

- CISA Tip: Best Practices for Securing Election Systems
- CISA Tip: Securing Voter Registration Data
- · CISA Tip: Website Security
- CISA Tip: Avoiding Social Engineering and Phishing Attacks
- CISA Tip: Securing Network Infrastructure Devices
- CISA Activity Alert: Technical Approaches to Uncovering and Remediating Malicious Activity
- CISA Insights: Actions to Counter Email-Based Attacks On Election-related Entities
- FBI and CISA Public Service Announcement (PSA): Spoofed Internet Domains and Email Accounts Pose Cyber and Disinformation Risks to Voters
- FBI and CISA PSA: Foreign Actors Likely to Use Online Journals to Spread Disinformation Regarding 2020 Elections
- FBI and CISA PSA: Distributed Denial of Service Attacks Could Hinder Access to Voting Information, Would Not Prevent Voting
- FBI and CISA PSA: False Claims of Hacked Voter Information Likely Intended to Cast Doubt on Legitimacy of U.S. Elections
- FBI and CISA PSA: Cyber Threats to Voting Processes Could Slow But Not Prevent Voting

FBI and CISA PSA: Foreign Actors and Cybercriminals Likely to Spread Disinformation Regarding 2020 Election Results TLP:WHITE

Contact Information

To report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contact your local FBI field office at www.fbi.gov/contact-us/field, or the FBI's 24/7 Cyber Watch (CyWatch) at (855) 292-3937 or by e-mail at CyWatch@fbi.gov. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. To request incident response resources or technical assistance related to these threats, contact CISA at Central@cisa.dhs.gov.

References

- [1] F5 Security Advisory: K52145254: TMUI RCE vulnerability CVE-2020-5902
- [2] Progress Telerik details for CVE-2017-9248
- [3] NSA "NSA'S Top Ten Cybersecurity Mitigation Strategies
- [4] OWASP Dependency-Check
- [5] NSA "Defending Against the Exploitation of SQL Vulnerabilities to Compromis....
- [6] NSA & ASD "CyberSecurity Information: Detect and Prevent Web Shell Malware"
- [7] CISA: Identifying and Protecting High Value Assets: A Closer Look at Govern...
- [8] NSA "NSA'S Top Ten Cybersecurity Mitigation Strategies"
- [9] NSA "Building Web Applications Security for Developers":
- [10] OWASP Top Ten
- [11] 2020 CWE Top 25 Most Dangerous Software Weaknesses

Revisions

October 22, 2020: Initial Version

This product is provided subject to this Notification and this Privacy & Use policy.



1580





Updated September 18, 2019

The Designation of Election Systems as Critical Infrastructure

Prior to the 2016 federal election, a series of cyberattacks occurred on information systems of state and local election jurisdictions. Subsequently, in January 2017 the Department of Homeland Security (DHS) designated the election infrastructure used in federal elections as a component of U.S. critical infrastructure. The designation sparked some initial concerns by state and local election officials about federal encroachment of their prerogatives, but progress has been made in overcoming those concerns and providing assistance to election jurisdictions.

What Led to the Designation?

In August 2016, the Federal Bureau of Investigation (FBI) announced that some state election jurisdictions had been the victims of cyberattacks aimed at exfiltrating data from information systems in those jurisdictions. The attacks appeared to be of Russian-government origin. That same month, DHS contacted state election officials to offer cybersecurity assistance for their election infrastructure. Most states accepted the offer. Although the cyberattacks did not appear to affect the integrity of the election infrastructure, some observers began calling for it to be designated as critical infrastructure (CI). On January 6, 2017, the Secretary of Homeland Security announced that designation.

What Is Critical Infrastructure?

Under federal law, CI refers to systems and assets for which "incapacity or destruction ... would have a debilitating impact on security, national economic security, national public health or safety, or any combination" of them (42 U.S.C. §5195e(e)). Most CI entities are not government-owned or -operated. Presidential Policy Directive 21(PPD 21) identified 16 CI sectors, with some including subsectors. Sectors vary in scope and in degree of regulation. For example, the financial services sector is highly regulated, whereas the information technology sector is not. Election infrastructure has been designated as a subsector of government facilities. That sector includes two previously established subsectors: education facilities, and national monuments and icons.

The Homeland Security Act of 2002 (P.L. 107-296) gave DHS responsibility for several functions aimed at promoting the security and resilience of CI with respect to both physical and cyber-based hazards, either human or natural in origin. Among those functions are providing assessments, guidance, and coordination of federal efforts.

Each CI sector has been assigned one or two federal sectorspecific agencies (SSAs), which are responsible for coordinating public/private collaborative efforts to protect the sector, including incident management and technical assistance. DHS has regulatory authority over two sectors: chemical and transportation systems. It serves as SSA for several, including the elections infrastructure subsector (EIS).

The components of the EIS as described by DHS include physical locations (storage facilities, polling places, and locations where votes are tabulated) and technology infrastructure (voter registration databases, voting systems, and other technology used to manage elections and to report and validate results). It does not include infrastructure related to political campaigns. However, DHS does provide cyber vulnerability assessments and risk mitigation guidance to political campaigns upon request as resources permit.

Does the Designation Permit Federal Regulation of Election Infrastructure?

DHS does not have regulatory authority over EIS. Five other agencies have significant roles with respect to federal elections, but none has claimed regulatory authority over the EIS:

- The Election Assistance Commission (EAC), created by the Help America Vote Act (HAVA, P.L. 107-252), provides a broad range of assistance to states, including development of voluntary technical standards for voting systems, voluntary guidance on implementing HAVA requirements, and research on issues in election administration. It also has statutory authority for administering formula payments to states to assist them in meeting HAVA requirements and improving election administration, including \$380 million appropriated in FY2018 in response to security concerns.
- The National Institute of Standards and Technology (NIST) assists the EAC on technical matters, including development of the voting system standards, certification of voting systems, and research.
- The Department of Justice (DOJ) has some enforcement responsibilities with respect to requirements in HAVA and other relevant statutes.
- The Department of Defense (DOD) assists military and overseas voters.
- The Federal Election Commission (FEC) is responsible for enforcement of campaign finance law but is not involved in election administration by state and local jurisdictions.

HAVA expressly prohibits the EAC from issuing regulations of relevance to the CI designation, and it leaves the methods of implementation of the act's requirements to the states. However, it does permit DOJ to bring civil actions if necessary to implement HAVA's requirements.

Case 1:21-cv-00040 Document 1-113 Filed 01/08/21 Page 23 of 215

The Designation of Election Systems as Critical Infrastructure

What Does the Designation Mean?

While both DHS and the EAC provided assistance to states in addressing the security concerns that arose in the run-up to the November 2016 election, the CI designation had several notable consequences:

- It raised the priority for DHS to provide security
 assistance to election jurisdictions that request it and for
 other executive branch actions, such as economic
 sanctions that the Department of the Treasury can
 impose against foreign actors who attack elements of
 U.S. CI, including tampering with elections.
- It brings the subsector under a 2015 United Nations nonbinding consensus report (A/70/174) stating that nations should not conduct or support cyber-activity that intentionally damages or impairs the operation of CI in providing services to the public. It also states that nations should take steps to protect their own CI from cyberattacks and to assist other nations in protecting their CI and responding to cyberattacks on it. The report was the work of a group of governmental experts from 20 nations, including Russia and the United States.
- It provided DHS the authority to establish formal coordination mechanisms for CI sectors and subsectors and to use existing entities to support the security of the subsector. Those mechanisms are used to enhance information sharing within the subsector and to facilitate collaboration within and across subsectors and sectors.
 For example, both the FBI and the Office of the Director of National Intelligence (ODNI) have participated in briefing election officials on threats to the EIS.

Among the coordination mechanisms for the subsector are the following:

- Government Coordinating Council. The GCC consists
 of representatives of DHS and the EAC, as well as
 secretaries of state, lieutenant governors, and elections
 officials who altogether represent 24 state and local
 governments. It also includes non-voting members from
 other relevant federal agencies. The GCC facilitates
 coordination across government entities both within EIS
 and in other sectors. Activities include communications,
 planning, issue resolution, and implementation of the
 security missions of the entities.
- Sector Coordinating Council. The SCC consists of representatives of nongovernment entities, most of which are providers of voting systems and other election-related products and services. SCCs are selforganized and self-governed. They are intended to represent private-sector interests and to facilitate collaboration activities, including information sharing, among the private-sector entities in the CI sector and with government entities.
- Sector-Specific Plan. Public- and private-sector partners have created SSPs for each of the 16 CI sectors. The plans are components of an overall National Infrastructure Protection Plan and provide a means for the sectors to establish goals and priorities for

addressing risks. They are generally updated on a fouryear cycle. DHS is currently drafting an SSP for the FIS

The CI designation for election infrastructure is also intended to facilitate use of existing resources, such as

- Cybersecurity and Infrastructure Security Agency (CISA). CISA, an agency within DHS, serves as the SSA for the EIS.
- Critical Infrastructure Partnership Advisory Council.
 CIPAC provides election officials access to a broad range of relevant expertise and participation in sensitive planning conversations.
- Multi-State Information Sharing and Analysis Center. The MS-ISAC is one of the centers created to facilitate the sharing of security information for different CI sectors. It works with CISA, all states, and many local governments to assist them in cybersecurity. The MS-ISAC supports the EIS-ISAC, created in 2018 to facilitate information-sharing activities for and among more than 500 members consisting of state and local election offices, as well as the National Association of Secretaries of State (NASS) and the National Association of State Election Directors (NASED).

Pursuant to the EIS designation, DHS and the EAC assisted both jurisdictions and vendors in preparations on election security for the 2018 federal election. For more information, see https://www.dhs.gov/topic/election-security, https://www.eac.gov/election-officials/elections-critical-infrastructure/, https://www.cisecurity.org/ei-isac/.

Why Was the Designation Initially Controversial?

Misgivings about DHS involvement were raised when it first offered assistance to election jurisdictions in August 2016. Some observers feared that DHS would begin to exert control over the administration of elections or to engage in unrequested security activities.

Controversy over the federal role in election administration is not new. Concerns about federal regulation of the election process were prominent during the legislative debate over HAVA and led to the inclusion of the regulatory restrictions in the law. Furthermore, bills in prior Congresses that would have provided DHS broad regulatory authority over cybersecurity have all failed.

The CI designation does not contravene the HAVA restrictions on EAC regulations or create DHS regulatory authority for the EIS. DHS provides assistance to election jurisdictions only on a voluntary basis. In the 115th Congress, a few bills would have established mandatory standards or federal rule-making authority, but none received committee or floor action. Bills with relevant provisions have also been introduced in the 116th Congress.

Brian E. Humphreys, bhumphreys@crs.loc.gov, 7-0975

IF10677



Alert (AA20-283A)

More Alerts

APT Actors Chaining Vulnerabilities Against SLTT, Critical Infrastructure, and Elections Organizations

Original release date: October 09, 2020 | Last revised: October 24, 2020

Summary

This joint cybersecurity advisory uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) framework. See the ATT&CK for Enterprise framework for all referenced threat actor techniques.

Note: the analysis in this joint cybersecurity advisory is ongoing, and the information provided should not be considered comprehensive. The Cybersecurity and Infrastructure Security Agency (CISA) will update this advisory as new information is available.

This joint cybersecurity advisory was written by CISA with contributions from the Federal Bureau of Investigation

CISA has recently observed advanced persistent threat (APT) actors exploiting multiple legacy vulnerabilities in combination with a newer privilege escalation vulnerability—CVE-2020-1472—in Windows Netlogon. The commonly used tactic, known as vulnerability chaining, exploits multiple vulnerabilities in the course of a single intrusion to compromise a network or application.

This recent malicious activity has often, but not exclusively, been directed at federal and state, local, tribal, and territorial (SLTT) government networks. Although it does not appear these targets are being selected because of their proximity to elections information, there may be some risk to elections information housed on government networks.

CISA is aware of some instances where this activity resulted in unauthorized access to elections support systems; however, CISA has no evidence to date that integrity of elections data has been compromised. There are steps that election officials, their supporting SLTT IT staff, and vendors can take to help defend against this malicious cyber activity.

Some common tactics, techniques, and procedures (TTPs) used by APT actors include leveraging legacy network access and virtual private network (VPN) vulnerabilities in association with the recent critical CVE-2020-1472 Netlogon vulnerability. CISA is aware of multiple cases where the Fortinet FortiOS Secure Socket Layer (SSL) VPN vulnerability CVE-2018-13379 has been exploited to gain access to networks. To a lesser extent, CISA has also observed threat actors exploiting the MobileIron vulnerability CVE-2020-15505. While these exploits have been observed recently, this activity is ongoing and still unfolding.

After gaining initial access, the actors exploit CVE-2020-1472 to compromise all Active Directory (AD) identity services. Actors have then been observed using legitimate remote access tools, such as VPN and Remote Desktop. Protocol (RDP), to access the environment with the compromised credentials. Observed activity targets multiple sectors and is not limited to SLTT entities.

CISA recommends network staff and administrators review internet-facing infrastructure for these and similar vulnerabilities that have or could be exploited to a similar effect, including Juniper CVE-2020-1631, Pulse Secure CVE-2019-11510, Citrix NetScaler CVE-2019-19781, and Palo Alto Networks CVE-2020-2021 (this list is not considered exhaustive).

Click here for a PDF version of this report.



Technical Details TLP:WHITE

Initial Access

APT threat actors are actively leveraging legacy vulnerabilities in internet-facing infrastructure (Exploit Public-Facing Application [T1190], External Remote Services [T1133]) to gain initial access into systems. The APT actors appear to have predominately gained initial access via the Fortinet FortiOS VPN vulnerability CVE-2018-13379.

Although not observed in this campaign, other vulnerabilities, listed below, could be used to gain network access (as analysis is evolving, these listed vulnerabilities should not be considered comprehensive). As a best practice, it is critical to patch all known vulnerabilities within internet-facing infrastructure.

- Citrix NetScaler CVE-2019-19781
- MobileIron CVE-2020-15505
- Pulse Secure CVE-2019-11510
- Palo Alto Networks CVE-2020-2021
- F5 BIG-IP CVE-2020-5902

Fortinet FortiOS SSL VPN CVE-2018-13379

CVE-2018-13379 is a path traversal vulnerability in the FortiOS SSL VPN web portal. An unauthenticated attacker could exploit this vulnerability to download FortiOS system files through specially crafted HTTP resource requests.

[1]

MobileIron Core & Connector Vulnerability CVE-2020-15505

CVE-2020-15505 is a remote code execution vulnerability in MobileIron Core & Connector versions 10.3 and earlier.

[2] This vulnerability allows an external attacker, with no privileges, to execute code of their choice on the vulnerable system. As mobile device management (MDM) systems are critical to configuration management for external devices, they are usually highly permissioned and make a valuable target for threat actors.

Privilege Escalation

Post initial access, the APT actors use multiple techniques to expand access to the environment. The actors are leveraging CVE-2020-1472 in Windows Netlogon to escalate privileges and obtain access to Windows AD servers. Actors are also leveraging the opensource tools such as Mimikatz and the CrackMapExec tool to obtain valid account credentials from AD servers (Valid Accounts [T1078]).

Microsoft Netlogon Remote Protocol Vulnerability: CVE-2020-1472

CVE-2020-1472 is a vulnerability in Microsoft Windows Netlogon Remote Protocol (MS-NRPC), a core authentication component of Active Directory.[3] This vulnerability could allow an unauthenticated attacker with network access to a domain controller to completely compromise all AD identity services (Valid Accounts: Domain Accounts [T1078.002]). Malicious actors can leverage this vulnerability to compromise other devices on the network (Lateral Movement [TA0008]).

Persistence

Once system access has been achieved, the APT actors use abuse of legitimate credentials (Valid Accounts [T1078]) to log in via VPN or remote access services (External Remote Services [T1133]) to maintain persistence.

Mitigations

Organizations with externally facing infrastructure devices that have the vulnerabilities listed in this joint cybersecurity advisory, or other vulnerabilities, should move forward with an "assume breach" mentality. As initial exploitation and escalation may be the only observable exploitation activity, most mitigations will need to focus on more traditional network hygiene and user management activities.

Keep Systems Up to Date



1584

Patch systems and equipment promptly and diligently. Establishing and consistently maintaining a thorough patching cycle continues to be the best defense against adversary TTPs. See table 1 for patch information on CVEs mentioned in this report.



Table 1: Patch information for CVEs

Vulnerability	Vulnerable Products	Patch Information	
CVE-2018-13379	 FortiOS 6.0: 6.0.0 to 6.0.4 FortiOS 5.6: 5.6.3 to 5.6.7 FortiOS 5.4: 5.4.6 to 5.4.12 	Fortinet Security Advisory: FG-IR-18-384	
CVE-2019-19781	Citrix Application Delivery Controller Citrix Gateway Citrix SDWAN WANOP	 Citrix blog post: firmware updates for Citrix ADC and Citrix Gate way versions 11.1 and 12.0 Citrix blog post: security updates for Citrix SD-WAN WANOP rele ase 10.2.6 and 11.0.3 Citrix blog post: firmware updates for Citrix ADC and Citrix Gate way versions 12.1 and 13.0 Citrix blog post: firmware updates for Citrix ADC and Citrix Gate way version 10.5 	
CVE-2020-5902	Big-IP devices (LTM, AAM, Advanced WAF, AF M, Analytics, APM, ASM, DDHD, DNS, FPS, GT M, Link Controller, PEM, SSLO, CGNAT)	F5 Security Advisory: K52145254: TMUI RCE vulnerability CVE-20 20-5902	
CVE-2019-11510	 Pulse Connect Secure 9.0R1 - 9.0R3.3, 8.3R1 - 8.3R7, 8.2R1 - 8.2R12, 8.1R1 - 8.1R15 Pulse Policy Secure 9.0R1 - 9.0R3.1, 5.4R1 - 5.4R7, 5.3R1 - 5.3R12, 5.2R1 - 5.2R12, 5.1R1 - 5.1R15 	Pulse Secure Out-of-Cycle Advisory: Multiple vulnerabilities reso lved in Pulse Connect Secure / Pulse Policy Secure 9.0RX	
CVE-2020-15505	 MobileIron Core & Connector versions 10,3.0. 3 and earlier, 10.4.0.0, 10.4.0.1, 10.4.0.2, 10.4. 0.3, 10.5.1.0, 10.5.2.0 and 10.6.0.0 Sentry versions 9.7.2 and earlier, and 9.8.0; Monitor and Reporting Database (RDB) version 2.0.0.1 and earlier 	MobileIron Blog: MobileIron Security Updates Available	
CVE-2020-1631	 Junos OS 12.3, 12.3X48, 14.1X53, 15.1, 15.1X4 9, 15.1X53, 17.2, 17.3, 17.4, 18.1, 18.2, 18.3, 1 8.4, 19.1, 19.2, 19.3, 19.4, 20.1 	Juniper Security Advisory JSA11021	
CVE-2020-2021	PAN-OS 9.1 versions earlier than PAN-OS 9.1. 3; PAN-OS 9.0 versions earlier than PAN-OS 9. 0.9; PAN-OS 8.1 versions earlier than PAN-OS 8.1.15, and all versions of PAN-OS 8.0 (EOL)	Palo Alto Networks Security Advisory for CVE-2020-2021	

1585

Vulnerability	Vulnerable Products	Patch Information	TLP:WHITE
VE-2020-1472	 Windows Server 2008 R2 for x64-based Syste ms Service Pack 1 Windows Server 2008 R2 for x64-based Syste ms Service Pack 1 (Server Core installation) Windows Server 2012 Windows Server 2012 (Server Core installation) Windows Server 2012 R2 Windows Server 2016 Windows Server 2019 Windows Server 2019 (Server Core installation) Windows Server, version 1903 (Server Core installation) Windows Server, version 1909 (Server Core installation) Windows Server, version 2004 (Server Core installation) Windows Server, version 2004 (Server Core installation) 	Microsoft Security Advisory for CVE-2020	

Comprehensive Account Resets

If there is an observation of CVE-2020-1472 Netlogon activity or other indications of valid credential abuse detected, it should be assumed the APT actors have compromised AD administrative accounts, the AD forest should not be fully trusted, and, therefore, a new forest should be deployed. Existing hosts from the old compromised forest cannot be migrated in without being rebuilt and rejoined to the new domain, but migration may be done through "creative destruction," wherein as endpoints in the legacy forest are decommissioned, new ones can be built in the new forest. This will need to be completed on on-premise as well as Azure-hosted AD instances.

Note that fully resetting an AD forest is difficult and complex; it is best done with the assistance of personnel who have successfully completed the task previously.

It is critical to perform a full password reset on all user and computer accounts in the AD forest. Use the following steps as a guide.

- 1. Create a temporary administrator account, and use this account only for all administrative actions
- 2. Reset the Kerberos Ticket Granting Ticket (krbtgt) password [4]; this must be completed before any additional actions (a second reset will take place in step 5)
- Wait for the krbtgt reset to propagate to all domain controllers (time may vary)
- Reset all account passwords (passwords should be 15 characters or more and randomly assigned):
 - User accounts (forced reset with no legacy password reuse)
 - b. Local accounts on hosts (including local accounts not covered by Local Administrator Password Solution [LAPS]]
 - c. Service accounts
 - d. Directory Services Restore Mode (DSRM) account
 - e. Domain Controller machine account
 - f. Application passwords
- 5. Reset the krbtgt password again
- 6. Wait for the krbtgt reset to propagate to all domain controllers (time may vary)
- 7. Reboot domain controllers
- 8. Reboot all endpoints

The following accounts should be reset:

- AD Kerberos Authentication Master (2x)
- All Active Directory Accounts
- All Active Directory Admin Accounts
- All Active Directory Service Accounts

- · All Active Directory User Accounts
- · DSRM Account on Domain Controllers
- Non-AD Privileged Application Accounts
- Non-AD Unprivileged Application Accounts
- Non-Windows Privileged Accounts
- Non-Windows User Accounts
- Windows Computer Accounts
- Windows Local Admin

CVE-2020-1472

To secure your organization's Netlogon channel connections:

- Update all Domain Controllers and Read Only Domain Controllers. On August 11, 2020, Microsoft released software updates to mitigate CVE-2020-1472. Applying this update to domain controllers is currently the only mitigation to this vulnerability (aside from removing affected domain controllers from the network).
- Monitor for new events, and address non-compliant devices that are using vulnerable Netlogon secure channel connections.
- Block public access to potentially vulnerable ports, such as 445 (Server Message Block [SMB]) and 135 (Remote Procedure Call [RPC]).

To protect your organization against this CVE, follow advice from Microsoft, including:

- Update your domain controllers with an update released August 11, 2020, or later.
- Find which devices are making vulnerable connections by monitoring event logs.
- Address non-compliant devices making vulnerable connections.
- Enable enforcement mode to address CVE-2020-1472 in your environment.

VPN Vulnerabilities

Implement the following recommendations to secure your organization's VPNs:

- · Update VPNs, network infrastructure devices, and devices being used to remote into work environments with the latest software patches and security configurations. See CISA Tips Understanding Patches and Software Updates and Securing Network Infrastructure Devices. Wherever possible, enable automatic updates. See table 1 for patch information on VPN-related CVEs mentioned in this report.
- Implement multi-factor authentication (MFA) on all VPN connections to increase security. Physical security tokens are the most secure form of MFA, followed by authenticator app-based MFA. SMS and email-based MFA should only be used when no other forms are available. If MFA is not implemented, require teleworkers to use strong passwords. See CISA Tips Choosing and Protecting Passwords and Supplementing Passwords for more information.

Discontinue unused VPN servers. Reduce your organization's attack surface by discontinuing unused VPN servers, which may act as a point of entry for attackers. To protect your organization against VPN vulnerabilities:

- Audit configuration and patch management programs.
- Monitor network traffic for unexpected and unapproved protocols, especially outbound to the internet (e.g., Secure Shell [SSH], SMB, RDP).
- Implement MFA, especially for privileged accounts.
- Use separate administrative accounts on separate administration workstations.
- Keep software up to date. Enable automatic updates, if available.

How to uncover and mitigate malicious activity

- Collect and remove for further analysis:
 - · Relevant artifacts, logs, and data.
- Implement mitigation steps that avoid tipping off the adversary that their presence in the network has been discovered.
- Consider soliciting incident response support from a third-party IT security organization to: Provide subject matter expertise and technical support to the incident response.

 Case 1:21-cv-00317-DCLC-CHS Document 22-7 Filed 01/20/22 Page 29 of 591 P



- Ensure that the actor is eradicated from the network.
- Avoid residual issues that could result in follow-up compromises once the incident is closed.

Resources

- CISA VPN-Related Guidance
- CISA Infographic: Risk Vulnerability And Assessment (RVA) Mapped to the MITRE ATT&CK FRAMEWORK
- National Security Agency InfoSheet: Configuring IPsec Virtual Private Networks
- CISA Joint Advisory: AA20-245A: Technical Approaches to Uncovering and Remediating Malicious Activity
- CISA Activity Alert: AA20-073A: Enterprise VPN Security
- CISA Activity Alert: AA20-031A: Detecting Citrix CVE-2019-19781
- CISA Activity Alert: AA20-010A: Continued Exploitation of Pulse Secure VPN Vulnerability
- Cybersecurity Alerts and Advisories: Subscriptions to CISA Alerts and MS-ISAC Advisories.

Contact Information

Recipients of this report are encouraged to contribute any additional information that they may have related to this threat.

For any questions related to this report or to report an intrusion and request resources for incident response or technical assistance, please contact:

- CISA (888-282-0870 or Central@cisa.dhs.gov), or
- The FBI through the FBI Cyber Division (855-292-3937 or CyWatch@fbi.gov) or a local field office

DISCLAIMER

This information is provided "as is" for informational purposes only. The United States Government does not provide any warranties of any kind regarding this information. In no event shall the United States Government or its contractors or subcontractors be liable for any damages, including but not limited to, direct, indirect, special or consequential damages, arising out of, resulting from, or in any way connected with this information, whether or not based upon warranty, contract, tort, or otherwise, whether or not arising out of negligence, and whether or not injury was sustained from, or arose out of the results of, or reliance upon the information.

The United States Government does not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply their endorsement, recommendation, or favoring by the United States Government.

References

- [1] Fortinet Advisory: FG-IR-18-384
- [2] Mobiletron Blog: Mobiletron Security Updates Available
- [3] Microsoft Security Advisory for CVE-2020-1472
- [4] Microsoft: AD Forest Recovery Resetting the krbtgt password

Revisions

October 9, 2020: Initial Version October 11, 2020: Updated Summary October 12, 2020: Added Additional Links

This product is provided subject to this Notification and this Privacy & Use policy.

Press Releases

Treasury Continues Pressure on Maduro Regime for Role in Fraudulent Elections

December 18, 2020

Washington – Today, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) designated Ex-Cle Soluciones Biometricas C.A. (Ex-Cle C.A.) for materially supporting the illegitimate President of Venezuela Nicolas Maduro Moros, including by providing goods and services that the Maduro regime used to carry out the fraudulent December 6, 2020 parliamentary elections. In addition, OFAC designated Guillermo Carlos San Agustin and Marcos Javier Machado Requena for having acted for or on behalf of Ex-Cle Soluciones Biometricas C.A.

"The illegitimate Maduro regime's efforts to steal elections in Venezuela show its disregard for the democratic aspirations of the Venezuelan people," said Secretary Steven T. Mnuchin. "The United States remains committed to targeting the Maduro regime and those who support its aim to deny the Venezuelan people their right to free and fair elections."

This entity and individuals were designated pursuant to Executive Order (E.O.) 13692, as amended.

EX-CLE SOLUCIONES BIOMETRICAS C.A.

Ex-Cle Soluciones Biometricas C.A. (Ex-Cle C.A.), a Venezuelan-registered biometric technology company, operates in Venezuela as the subsidiary of Argentine-registered Ex-Cle S.A. The parent company opened an office in Venezuela in 2004 to provide management solutions for government entities, including to Maduro's National Electoral Council (CNE – Consejo Nacional Electoral). In May 2016, the parent company began operating in Venezuela under the name Ex-Cle C.A., and since then, Ex-Cle C.A. has been doing business as the electoral hardware and software vendor with Maduro regime-aligned government agencies and officials. In addition, Ex-Cle C.A. has assisted the CNE in purchasing thousands of voting machines from foreign vendors, which were transshipped through Tehran, Iran, via Mahan Air and Conviasa, both previously sanctioned by OFAC. Ex-Cle C.A. has contracts worth millions of dollars with the Maduro regime.

GUILLERMO CARLOS SAN AGUSTIN

Guillermo Carlos San Agustin (San Agustin), a dual Argentine and Italian national, is a codirector, the administrator, a majority shareholder, and ultimate beneficial owner of Ex-Cle C.A. San Agustin is partnered in Ex-Cle C.A. with Marcos Javier Machado Requena, a Venezuelan national, and Carlos Enrique Quintero Cuevas (Quintero), previously designated by OFAC, who is an alternate CNE rector and member of the Venezuelan military, and is the primary day-to-day manager of the procurement and electoral corruption activity from inside the CNE on behalf of Ex-Cle C.A.

MARCOS JAVIER MACHADO REQUENA

Marcos Javier Machado Requena (Machado), a Venezuelan national, is a co-director, the president, and a minority shareholder of Ex-Cle C.A. Machado is involved in the management and financial operations of procurement of election-related voting machines and hardware procured from foreign vendors for the Government of Venezuela, and is partnered with San Agustin and Quintero in running Ex-Cle C.A. out of Caracas.

Today, Ex-Cle C.A. was designated pursuant to E.O. 13692 for having materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, Maduro. In addition, San Agustin and Machado were designated pursuant to E.O. 13692 for having acted or purported to act for or on behalf of, directly or indirectly, Ex-Cle C.A.

As a result of today's action, all property and interests in property of the persons designated today that are in the United States or in the possession or control of U.S. persons are blocked and must be reported to OFAC. In addition, any entities that are owned, directly or indirectly, 50 percent or more by the designated persons are also blocked. OFAC's regulations generally prohibit all dealings by U.S. persons or those within (or transiting) the United States that involve any property or interests in property of blocked or designated persons.

U.S. sanctions need not be permanent; sanctions are intended to bring about a positive change of behavior. The United States has made clear that the removal of sanctions may be available for individuals and entities, including those designated pursuant to E.O. 13692, who take concrete and meaningful actions to stop providing support to the illegitimate Maduro regime, including to those Government of Venezuela agencies that support him.

View identifying information on the entity designated today.

116TH CONGRESS 1st Session SENATE

REPORT 116-XX

REPORT

OF THE

SELECT COMMITTEE ON INTELLIGENCE UNITED STATES SENATE

ON

RUSSIAN ACTIVE MEASURES CAMPAIGNS AND INTERFERENCE IN THE 2016 U.S. ELECTION

VOLUME 1: RUSSIAN EFFORTS AGAINST ELECTION

INFRASTRUCTURE

WITH ADDITIONAL VIEWS

CONTENTS

I. (U) INTRODUCTION	3
II. (U) FINDINGS	3
III. (U) THE ARC OF RUSSIAN ACTIVITIES	5
IV. (U) ELEMENTS OF RUSSIAN ACTIVITIES	10
A. (U) Targeting Activity	10
B. (U) Russian Access to Election Infrastructure	21
(U) Russian Access to Election Infrastructure: Illinois	22
2. Russian Access to Election Infrastructure:	24
C. Russian Efforts to Research U.S. Voting Systems, Processes, and Other Elemen	its of
Voting Infrastructure	28
D. Russian Activity Directed at Voting Machine Companies	29
E. Russian Efforts to Observe Polling Places	30
F.	. 32
G. Russian Activity Possibly Related to a Misinformation Campaign on Vote	
77	. 32
H. (U) Two Unexplained Events	33
(U) Cyber Activity in State 22	. 33
2. (U) Cyber Activity in State 4	. 34
V. (U) RUSSIAN INTENTIONS	. 35
VI. (U) NO EVIDENCE OF CHANGED VOTES OR MANIPULATED VOTE TALLIES	. 38
VII. (U) SECURITY OF VOTING MACHINES	40
VIII. (U) THE ROLE OF DHS AND INTERACTIONS WITH THE STATES	
A. (U) DHS's Evolution	46
B. (U) The View From the States	49
C. (U) Taking Advantage of DHS Resources	52
X. (U) RECOMMENDATIONS	54

Russian Efforts Against Election Infrastructure

1. (U) INTRODUCTION

(U) From 2017 to 2019, the Committee held hearings, conducted interviews, and reviewed intelligence related to Russian attempts in 2016 to access election infrastructure. The Committee sought to determine the extent of Russian activities, identify the response of the U.S. Government at the state, local, and federal level to the threat, and make recommendations on how to better prepare for such threats in the future. The Committee received testimony from state election officials, Obama administration officials, and those in the Intelligence Community and elsewhere in the U.S. Government responsible for evaluating threats to elections.

II. (U) FINDINGS

1.	The Russian government directed extensive activity, beginning in at least 2014 and carrying into at least 2017, against U.S. election infrastructure at the state and local level.
2.	The Committee has seen no evidence that any votes were changed or that any voting machines were manipulated. ²

The Committee has reviewed the intelligence reporting underlying the Department of Homeland Security (DHS) assessment from early 2017

The Committee finds it credible.

³ (U) The names of the states the Committee spoke to have been replaced with numbers. DHS and some states asked the Committee to protect state names before providing the Committee with information. The Committee's goal was to get the most information possible, so state names are anonymized throughout this report. Where the report refers to public testimony by Illinois state election officials, that state is identified.

COMMITTEE SENSITIVE - RUSSIA INVESTIGATION ONLY

¹ (U) The Department of Homeland Security (DHS) defines election infrastructure as "storage facilities, polling places, and centralized vote tabulation locations used to support the election process, and information and communications technology to include voter registration databases, voting machines, and other systems to manage the election process and report and display results on behalf of state and local governments, "according to the January 6, 2017 statement issued by Secretary of Homeland Security Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector, available at https://www.dhs.gov/news/2017/10/06/statement-secretary-johnson-designation-election-infrastructure-critical. Similarly, the Help America Vote Act (HAVA), Pub. L. No. 107-252, Section 301(b)(1) refers to a functionally similar set of equipment as "voting systems," although the definition excludes physical polling places themselves, among other differences, 52 U.S.C. §21081(b). This report uses the term election infrastructure broadly, to refer to the equipment, processes, and systems related to voting, tabulating, reporting, and registration.

- (U) While the Committee does not know with confidence what Moscow's intentions
 were, Russia may have been probing vulnerabilities in voting systems to exploit later.
 Alternatively, Moscow may have sought to undermine confidence in the 2016 U.S.
 elections simply through the discovery of their activity.
- 4. (U) Russian efforts exploited the seams between federal authorities and capabilities, and protections for the states. The U.S. intelligence apparatus is, by design, foreign-facing, with limited domestic cybersecurity authorities except where the Federal Bureau of Investigation (FBI) and the Department of Homeland Security (DHS) can work with state and local partners. State election officials, who have primacy in running elections, were not sufficiently warned or prepared to handle an attack from a hostile nation-state actor.
- 5. (U) DHS and FBI alerted states to the threat of cyber attacks in the late summer and fall of 2016, but the warnings did not provide enough information or go to the right people. Alerts were actionable, in that they provided malicious Internet Protocol (IP) addresses to information technology (IT) professionals, but they provided no clear reason for states to take this threat more seriously than any other alert received.
- 6. (U) In 2016, officials at all levels of government debated whether publicly acknowledging this foreign activity was the right course. Some were deeply concerned that public warnings might promote the very impression they were trying to dispel—that the voting systems were insecure.
- 7. (U) Russian activities demand renewed attention to vulnerabilities in U.S. voting infrastructure. In 2016, cybersecurity for electoral infrastructure at the state and local level was sorely lacking; for example, voter registration databases were not as secure as they could have been. Aging voting equipment, particularly voting machines that had no paper record of votes, were vulnerable to exploitation by a committed adversary. Despite the focus on this issue since 2016, some of these vulnerabilities remain.
- 8. (U) In the face of this threat and these security gaps, DHS has redoubled its efforts to build trust with states and deploy resources to assist in securing elections. Since 2016, DHS has made great strides in learning how election procedures vary across states and how federal entities can be of most help to states. The U.S. Election Assistance Commission (EAC), the National Association of Secretaries of State (NASS), the National Association of State Election Directors (NASED), and other groups have helped DHS in this effort. DHS's work to bolster states' cybersecurity has likely been effective, in particular for those states that have leveraged DHS's cybersecurity assessments for election infrastructure, but much more needs to be done to coordinate state, local, and federal knowledge and efforts in order to harden states' electoral infrastructure against foreign meddling.
- (U) To assist in addressing these vulnerabilities, Congress in 2018 appropriated \$380 million in grant money for the states to bolster cybersecurity and replace vulnerable

voting machines.4 When those funds are spent, Congress should evaluate the results and consider an additional appropriation to address remaining insecure voting machines and systems.

10. (U) DHS and other federal government entities remain respectful of the limits of federal involvement in state election systems. States should be firmly in the lead for running elections. The country's decentralized election system can be a strength from a cybersecurity perspective, but each operator should be keenly aware of the limitations of their cybersecurity capabilities and know how to quickly and properly obtain assistance.

III. (U) THE ARC OF RUSSIAN ACTIVITIES
In its review of the 2016 elections, the Committee found no evidence that vote tallies were altered or that voter registry files were deleted or modified, though the Committee and IC's insight into this is limited. Russian government-affiliated cyber actors conducted an unprecedented level of activity against state election infrastructure in the run-up to the 2016 U.S. elections
Throughout 2016 and for several years before, Russian intelligence services and government personnel conducted a number of intelligence-related activities
targeting the voting process. the Committee found ample evidence to suggest
that the Russian government was developing and implementing capabilities to interfere in the 2016 elections, including undermining confidence in U.S. democratic institutions and voting processes. ⁵
Charles and the same of the sa
THE RESERVE THE PARTY OF THE PA
(U) Consolidated Appropriations Act, 2018, Pub. L. No. 115-141, 132 Stat. 348, 561-562. (U) The Committee has limited information on the extent to which state and local election authorities carried out forensic evaluation of registration databases. These activities are routinely carried out in the context of private sector breaches.
FBI LHM, FBI LHM, BUTTON DHS Homeland Intelligence Brief,
TEBLICHM,
5
COMMITTEE SENSITIVE - RUSSIA INVESTIGATION ONLY

THE RESIDENCE OF THE PARTY OF T
1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1
Evidence of scanning of state election systems first appeared in the summer prior to the 2016 election. In mid-July 2016, Illinois discovered anomalous network activity, specifically a large increase in outbound data, on a Illinois Board of Elections' voter registry website. Working with Illinois, the FBI commenced an investigation. 13
The attack resulted in data exfiltration from the voter registration database. 16
(U) On August 18, 2016, FBI issued an unclassified FLASH ¹⁷ to state technical-level experts on a set of suspect IP addresses identified from the attack on Illinois's voter registration databases. ¹⁸
The FLASH product did not attribute the attack to Russia or any other particular actor. ²¹
FBI LHM, (U) DHS briefing for SSCI staff, March 5, 2018. (U) SSCI Transcript of the Open Hearing on Russian Interference in the 2016 U.S. Elections, held on Wednesday, June 21, 2017, p. 113.
According to the United States Computer Emergency Readiness Team (US-CERT), an SQL injection is "an echnique that attempts to subvert the relationship between a webpage and its supporting database, typically in order to trick the database into executing malicious code."
(U) DHS IIR 4 0050006 17, An IP Address Targeted Multiple U.S. State Government's to Include Election Systems, October 4, 2016
(U) PBI FLASH alerts are notifications of potential cyber threats sent to local law enforcement and private industry so that administrators are able to guard their systems against the described threat. FLASHs marked TLP: AMBER are considered sharable with members of the recipients own organization and those with direct need to know.
Number T-LD1004-TT, TLP-AMBER, 9 (U) Ibid.
20 (U) 1bid.
wned
COMMITTEE SENSITIVE - RUSSIA INVESTIGATION ONLY

(U) After the issuance of the August FLASH, the Department of Homeland Security (DHS) and the Multi-State-Information Sharing & Analysis Center (MS-ISAC)²² asked states to review their log files to determine if the IP addresses described in the FLASH had touched their infrastructure. This request for voluntary self-reporting, in conjunction with DHS analysis of NetFlow activity on MS-ISAC internet sensors, identified another 20 states whose networks had made connections to at least one IP address listed on the FLASH.²³ DHS was almost entirely reliant on states to self-report scanning activity.

Former Special Assistant to the President and Cybersecurity Coordinator Michael Daniel said, "eventually we get enough of a picture that we become confident over the course of August of 2016 that we're seeing the Russians probe a whole bunch of different state election infrastructure, voter registration databases, and other related infrastructure on a regular basis." Dr. Samuel Liles, Acting Director of the Cyber Analysis Division within DHS's Office of Intelligence and Analysis (I&A), testified to the Committee on June 21, 2017, that "by late September, we determined that internet-connected election-related networks in 21 states were potentially targeted by Russian government cyber actors." 26



²² (U) The MS-ISAC is a DHS-supported group dedicated to sharing information between state, local, tribal, and territorial (SLTT) government entities. It serves as the central cybersecurity resource for SLTT governments. Entities join to receive cybersecurity advisories and alerts, vulnerability assessments, incident response assistance, and other services.

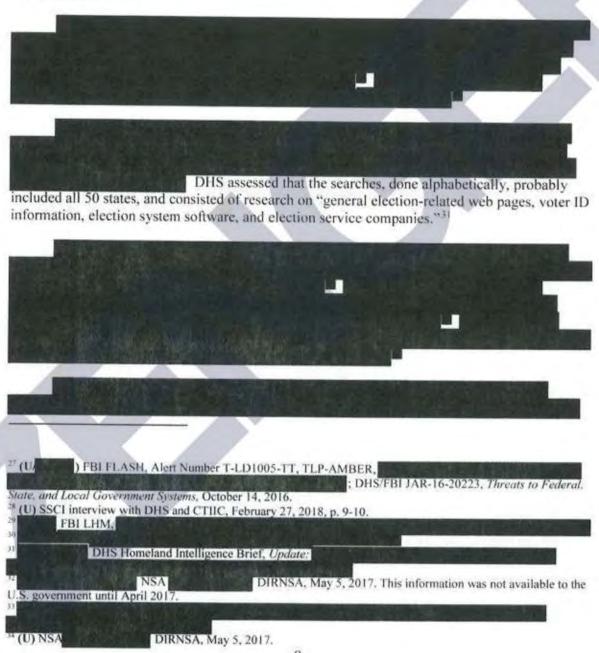
²³ (U) DHS IIR 4 005 0006, An IP Address Targeted Multiple U.S. State Governments to Include Election Systems, October 4, 2016; DHS briefing for SSC1 staff, March 5, 2018.

²⁴ (U) SSCI Transcript of the Interview with John Brennan, Former Director, CIA, held on Friday, June 23, 2017, p. 41.

²⁵ (U) SSCI Transcript of the Interview with Michael Daniel, Former Special Assistant to the President and Cybersecurity Coordinator, National Security Council, held on August 31, 2017, p. 39.

²⁶ (U) SSCI Transcript of the Open Hearing on Russian Interference in the 2016 U.S. Elections, held on Wednesday, June 21, 2017, p. 12.

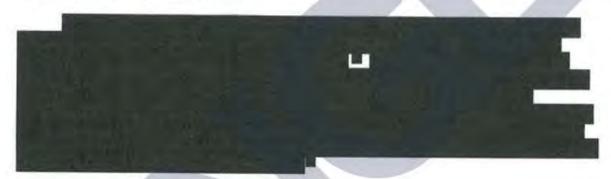
(U) DHS and FBI issued a second FI ASH and a Joint Analysis Report in October that flagged suspect IP addresses, many unrelated to Russia. 27 DHS briefers told the Committee that they were intentionally over-reporting out of an abundance of caution, given their concern about the seriousness of the threat. DHS representatives told the Committee, "We were very much at that point in a sort of duty-to-warn type of attitude . . . where maybe a specific incident like this, which was unattributed at the time, wouldn't have necessarily risen to that level. But . . . we were seeing concurrent targeting of other election-related and political figures and political institutions . . . [which] led to what would probably be more sharing than we would normally think to do." 28



Russian Embassy placed a formal request to observe the elections with the Department of State, but also reached outside diplomatic channels in an attempt to secure permission directly from state and local election officials. 37 In objecting to these tactics, then-Assistant Secretary of State for European and Eurasian Affairs Victoria Nuland reminded the Russian Ambassador that Russia had refused invitations to participate in the official OSCE mission that was to observe the U.S. elections. 38 35 (U) FBI IIR ; FBL IIR 16 (U) Ibid. U) DTS 2018-2152, SSCI Interview with Andrew McCabe, Former Deputy Director of the FBI, February 14, 2018, pp. 221-222. Email, sent November 4, 2016; from ; to: Subject: Kislyak Protest of FBI Tactics. (U) NSA DIRNSA, May 5, 2017. (U) Ibid. COMMITTEE SENSITIVE - RUSSIA INVESTIGATION ONLY

(U) The Committee found no evidence of Russian actors attempting to manipulate vote tallies on Election Day, though again the Committee and IC's insight into this is limited.

(U/Line 1) In the years since the 2016 election, awareness of the threat, activity by DHS, and measures at the state and local level to better secure election infrastructure have all shown considerable improvement. The threat, however, remains imperfectly understood. In a briefing before Senators on August 22, 2018, DNI Daniel Coats, FBI Director Christopher Wray, then-DHS Secretary Kirstjen Nielsen, and then-DHS Undersecretary for the National Protection and Programs Division Christopher Krebs told Senators that there were no known threats to election infrastructure. However, Mr. Krebs also said that top election vulnerabilities remain, including the administration of the voter databases and the tabulation of the data, with the latter being a much more difficult target to attack. Relatedly, several weeks prior to the 2018 mid-term election, DHS assessed that "numerous actors are regularly targeting election infrastructure, likely for different purposes, including to cause disruptive effects, steal sensitive data, and undermine confidence in the election." 45



IV. (U) ELEMENTS OF RUSSIAN ACTIVITIES

A. (U) Targeting Activity

Scanning of election-related state infrastructure by Moscow was the most widespread activity the IC and DHS elements observed in the run up to the 2016 election. 48

In an interview with the Committee, Mr. Daniel stated: "What it mostly looked like to us was reconnaissance. . . . I would have characterized it at the time as sort of conducting the reconnaissance to do the network mapping, to do the topology mapping so

45 (U) Homeland Security Intelligence Assessment: Cyber Actors Continue to Engage in Influence Activities and Targeting of Election Infrastructure, October 11, 2018:

^{44 (}U) DTS 2018-3275, Summary of 8/22/2018 All Senators Election Security Briefing, August 28, 2018.

⁴⁶ (U) DTS 2019-1368, NIC 2019-01, Intelligence Community Assessment: A Summary of the Intelligence Community Report on Foreign Interference as Directed by Executive Order 13848, March 29, 2019. p. 2-3.
⁴⁷ (U) Ibid.

^{48 (}U) SSCI interview of representatives from DHS and CTIIC, February 27, 2018, p. 12.

that you could actually understand the network, establish a presence so you could come back later and actually execute an operation." ¹⁹

(U) Testifying before the Committee, Dr. Liles characterized the activity as "simple scanning for vulnerabilities, analogous to somebody walking down the street and looking to see if you are home. A small number of systems were unsuccessfully exploited, as though somebody had rattled the doorknob but was unable to get in . . [however] a small number of the networks were successfully exploited. They made it through the door."50

DHS and FBI assessments on the number 2016. In a joint FBI/DHS intelligence product published in Ma	arch 2018, and coordinated with
the Central Intelligence Agency (CIA), the Defense Intelligence of State, the National Intelligence Council, the National Securit	e Agency (DIA), the Department
Department of Treasury, DHS and FBI assessed services conducted activity	that Russian intelligence

- DHS arrived at their initial assessment by evaluating whether the tactics, techniques, and procedures (TTPs) observed were consistent with previously observed Russian TTPs, whether the actors used known Russian-affiliated malicious infrastructure, and whether a state or local election system was the target.
- (U) The majority of information examined by DHS was provided by the states themselves. The MS-ISAC gathered information from states that noticed the suspect IPs pinging their systems. In addition, FBI was working with some states in local field offices and reporting back FBI's findings.
- (U) If some states evaluated their logs incompletely or inaccurately, then DHS might have no indication of whether they were scanned or attacked. As former-Homeland Security Adviser Lisa Monaco told the Committee, "Of course, the law enforcement and the intelligence community is going to be significantly reliant on what the holders and

⁴⁹ (U) SSCI Transcript of the Interview of Michael Daniel, Former Assistant to the President and Cybersecurity Coordinator, National Security Council, August 31, 2017, p. 44.

^{50 (}U) SSCI Transcript of the Open Hearing on Russian Interference in the 2016 U.S. Elections, held on Wednesday, June 21, 2017, p. 13.

DHS/FBI Homeland Intelligence Brief,

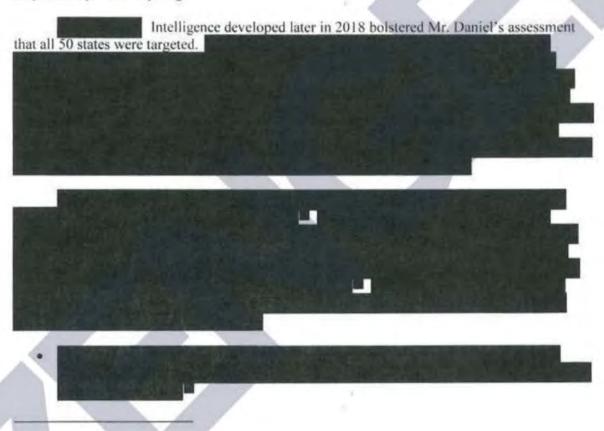
² (U) See chart, infra, for information on successful breaches.

^{53 (}U) DHS did not count attacks on political parties, political organizations, or NGOs. For example, the compromise of an email affiliated with a partisan State 13 voter registration organization was not included in DHS's count.

owners and operators of the infrastructure sees on its system [sic] and decides to raise their hand."54

However, both the IC and the Committee in its own review were unable to discern a pattern in the affected states,

(U) Mr. Daniel told the Committee that by late August 2016, he had already personally concluded that the Russians had attempted to intrude in all 50 states, based on the extent of the activity and the apparent randomness of the attempts. "My professional judgment was we have to work under the assumption that they've tried to go everywhere, because they're thorough, they're competent, they're good."55



^{54 (}U) SSCI Transcript of the Interview with of Lisa Monaco, Former Homeland Security Advisor, August 10, 2017, p. 38.

DHS/FBI Homeland Intelligence Bulletin,

12

¹⁵ (U) SSCI Transcript of the Interview with Michael Daniel, Former Assistant to the President and Cybersecurity Coordinator, National Security Council, August 31, 2017, p. 40.

^{27 (}U) Ibid.

^{58 (}U) DHS briefing for SSCI staff, March 5, 2018.

⁵⁹ (U) SSCI interview of representatives from DHS and CTIIC, February 27, 2018, pp. 11-12.

^{60 (}U) DHS briefing for SSCI staff, March 5, 2018.



(U) However, IP addresses associated with the August 18, 2016 FLASH provided some indications the activity might be attributable to the Russian government, particularly the GRU;



• (U) One of the Netherlands-based
"exhibited the same behavior from the same node over a period of time. . . . It was
behaving like . . . the same user or group of users was using this to direct activity against
the same type of targets," according to DHS staff. 69



67 (U) Cyber Threat Intelligence Integration Center (CTIIC) Cyber Threat Intelligence Summary, October 7, 2016.
68 (U) Ibid.

^{69 (}U) SSCI interview of representatives from DHS and CTIIC, February 27, 2018, p. 13.

The IC's confidence level about the attribution of the attacks evolved over 2017 and into 2018.

The Committee reached out to the 21 states that DHS first identified as targets of scanning activity to learn about their experiences. Election officials provided the Committee

14

^{70 (}U) DHS Electronic Communication, December 19, 2016, email from: DHS/NCCIC; to: CIA.

DHS Intelligence Assessment, Hostile Russian Cyber Targeting of Election Infrastructure in 2016: Probable Non-State Actors Attempt Disruption, May 3, 2017.

74 (U) Ibid.

⁷⁵ (U) SSCI interview of representatives from DHS and CTIIC, February 27, 2018, p. 13.

To DHS arrived at their initial assessment of 21 states affected by adding the eleven plus seven states, plus the three where scanning activity appeared directed at less specifically election-focused infrastructure.

To (U) SSCI conference call with DHS and FBI, March 29, 2018.

details about the activity they saw on their networks, and the Committee compared that accounting to DHS's reporting of events. 78 Where those accounts differed is noted below. The scanning activity took place from approximately June through September 2016.

STATE	OBSERVED ACTIVITY79			
Illinois	(U) See infra, "Russian Access to Election-Related Infrastructure" for a detailed description.			
State 2	(U) See infra, "Russian Access to Election-Related Infrastructure" for a detailed description,			
State 3	(U) According to State 3 officials, cyber actors using infrastructure identified in the August FLASH conducted scanning activity. 80 State 3 officials noticed "abnormal behavior" and took action to block the related IP addresses. 81 DHS reported GRU scanning attempts against two separate domains related to election infrastructure. 82			
State 4	(U) See infra. "Two Unexplained Events" for a detailed description.			
State 5	(U) Cyber actors using infrastructure identified in the August FLASH scanned "an old website and non-relevant archives," according to the State 5 Secretary of State's office. The following day, State 5 took action to block the IP address. DHS, however, reported GRU scanning activity on two separate State 5 Secretary of State websites, plus targeting of a District Attorney's office sin a particular city. Both the websites appear to be current addresses for the State			
State 6	5 Secretary of State's office. (U) According to State 6 officials, cyber actors using infrastructure identifies the August FLASH scanned ⁸⁷ the entire state IT infrastructure, including by using the Acunetix tool, but the "affected systems" were the Secretary of States.			

^{78 (}U) DHS briefed Committee staff three times on the attacks, and staff reviewed hundreds of pages of intelligence assessments.

⁽U) Slight variation between what states and DHS reported to the Committee is an indication of one of the challenges in election cybersecurity. The system owners—in this case, state and local administrators—are in the best position to carry out comprehensive cyber reviews, but they often lack the expertise or resources to do so. The federal government has resources and expertise, but the IC can see only limited information about inbound attacks because of legal restrictions on operations inside the United States.

^{80 (}U) Memorandum for the Record, SSCI Staff, Conference Call with [State 3], December 8, 2017.

^{*) (}U) Ibid.

^{82 (}U) DHS briefing for Committee staff on March 5, 2018.

^{*1 (}U) Memorandum for the Record, SSCI Staff, Conference Call with [State 5], December 1, 2017.

^{84 (}U) Ibid.

Briefers suggested the "most wanted" list housed on the District Attorney's website may have in some way been connected to voter registration. The exact nature of this connection, including whether it was a technical network connection or whether databases of individuals with felony convictions held by the District Attorney's office had voting registration implications, is unclear.

^{86 (}U) DHS briefing for Committee staff on March 5, 2018.

^{87 (}U) State 6 officials did not specify, but in light of the DHS assessment, they likely meant SQL injection.

	web application and the election results website. 88 If the penetration had been successful, actors could have manipulated the unofficial display of the election tallies. 89 State officials believed they would have caught any inconsistency quickly. 90 State 6 became aware of this malicious activity and alerted partners. 91 DHS reported that GRU actors scanned State 6, then unsuccessfully
	attempted many SQL injection attacks. State 6 saw the highest number of SQL attempts of any state.
State 7	(U) According to State 7 officials, cyber actors using infrastructure identified in the August FLASH scanned public-facing websites, including the "static" election site. 92 It seemed the actors were "cataloging holes to come back later," according to state election officials. 93 State 7 became aware of this malicious activity after receiving an FBI alert. 94
	DHS reported GRU scanning attempts against two separate domains related to election infrastructure. 95
	(U) According to State 8 officials, cyber actors using infrastructure identified in the August FLASH scanned a State 8 public election website on one day. ⁹⁶ State 8 officials described the activity as heightened but not particularly out of the ordinary. ⁹⁷ State 8 became aware of this malicious activity after receiving an alert. ⁹⁸
State 8	
State 9	(U) According to State 9 officials, cyber actors using infrastructure identified in an October MS-ISAC advisory 101 scanned the statewide voter registration

^{88 (}U) Memorandum for the Record, SSCI Staff, Conference Call with [State 6], November 17, 2017.

^{89 (}U) Ibid.

^{90 (}U) Ibid.

[&]quot; (U) Ibid.

⁹⁷ (U) Memorandum for the Record, SSCI Staff, Conference Call with [State 7], January 25, 2018.

^{10 (}U) Ibid.

^{94 (}U) Ibid.

^{96 (}U) DHS briefing for Committee staff on March 5, 2018.

⁽U) Memorandum for the Record, SSCI Staff, Conference Call with [State 8], February 2, 2018.

^{97 (}U) Ibid.

^{95 (}U) Ibid.

⁽U) DHS briefing for Committee staff on March 5, 2018.

^{100 (}U) Ibid.

⁽U) While the Committee was unable to review the specific indicators shared with State 9 by the MS-ISAC in October, the Committee believes at least one of the relevant IPs was originally named in the August FLASH because of technical data held by DHS which was briefed to the Committee.

	system. 102 Officials used the analogy of a thief casing a parking lot: they said the car thief "didn't go in, but we don't know why." 103 State 9 became aware of this malicious activity after receiving an alert. 104 DHS reported GRU scanning activity on the Secretary of State domain. 105
State 10	(U) According to State 10 officials, cyber actors using infrastructure identified in the August FLASH conducted activity that was "very loud," with a three-pronged attack: a Netherlands-based IP address attempted SQL injection on all fields 1,500 times, a U.Sbased IP address attempted SQL injection on several fields, and a Poland-based IP address attempted SQL injection on one field 6-7 times. ¹⁰⁶ State 10 received relevant cybersecurity indictors from MS-ISAC in early August, around the same time that the attacks occurred. ¹⁰⁷ State 10's IT contractor attributed the attack to Russia and suggested that the activity was reminiscent of other attacks where attackers distract with lots of noise and then "sneak in the back." ¹⁰⁸ (U) State 10, through its firewall, blocked attempted malicious activity against the online voter registration system and provided logs to the National Cybersecurity and Communications Integration Center (NCCIC) ¹⁰⁹ and the U.S. Computer Emergency Readiness Team (US-CERT). ¹¹⁰ State 10 also brought in an outside contractor to assist. ¹¹¹
	DHS confirmed GRU SQL injection attempts against State 10's voter services website on August 5 and said that the attack was blocked after one day by State 10's firewall. 112
State 11	(U) According to State 11 officials, they have seen no evidence of scanning or attack attempts related to election infrastructure in 2016. While State 11 officials noted an IP address "probing" state systems, activity which was "broader than state election systems," State 11 election officials did not provide specifics on which systems.
F 1	

17

^{102 (}U) Memorandum for the Record, SSCI Staff, Conference Call with [State 9], November 17, 2017.

in (U) Ibid.

^{104 (}U) Ibid.

^{105 (}U) DHS briefing for Committee staff on March 5, 2018.

⁽U) Memorandum for the Record, SSCI Staff, Conference Call with [State 10], November 29, 2017.

^{10&}quot; (U) Ibid.

^{10% (}U) Ibid.

^{109 (}U) NCCIC is DHS's cyber watch center.

^{110 (}U) Ibid.

⁽U) Ibid.

^{112 (}U) DHS briefing for Committee staff on March 5, 2018.

^{113 (}U) Memorandum for the Record, SSCI Staff, Conference Call with [State 11], December 8, 2017.

^{114 (}U) Ibid.

	DHS reported GRU scanning activity on the Secretary of State
State 12	(U) Cyber actors using infrastructure identified in the August FLASH conducted scanning activity that "lasted less than a second and no security breach occurred," according to State 12 officials. 116 State 12 became aware of this malicious activity after being alerted to it. 117
	DHS reported that because of a lack of sensor data related to this incident, they relied on NetFlow data, which provided less granular information. DHS's only clear indication of GRU scanning on State 12's Secretary of State website came from State 12 self-reporting information to MS-ISAC after the issuance of the August FLASH notification. 119
	(U) According to State 13 officials, they have seen no evidence of scanning or attack attempts related to state-wide election infrastructure in 2016. 120
State 13	
State 14	MS-ISAC passed DHS reports of communications between a suspect IP address used by the GRU at the time and the State 14 election commission webpage, but no indication of a compromise. ¹²³ In addition, DHS was informed of activity relating to separate IP addresses in the August FLASH,

; DHS briefing for Committee

staff on March 5, 2018. For more information on decisions by DHS to exclude certain activity in its count of 21 states, see text box, infra, "DHS Methodology for Identifying States Touched by Russian Cyber Actors."

DHS/FBI Homeland Intelligence Brief,

; DHS briefing for Committee staff on March 5, 2018.

18

⁽U) DHS briefing for Committee staff on March 5, 2018.

^{116 (}U) Memorandum for the Record, SSCI Staff, Conference Call with [State 12], December 1, 2017.

^{117 (}U) Ibid.

^{118 (}U) DHS briefing for Committee staff on March 5, 2018.

^{190 (}U) Ibid.

^{120 (}U) Memorandum for the Record, SSCI Staff, Conference Call with [State 13], December 1, 2017.

⁽U) FBI IIR DHS briefing for Committee staff on March 5, 2018.

	including attempted Domain Name System (DNS) lookups and potentially malicious emails, some dating back to January 2016. 124		
State 15	(U) State 15 officials were not aware that the state was among those targeted until they were notified. 123 State 15 s current lead election official was not in place during the 2016 election so they had little insight into any scanning or attempted intrusion on their systems. State 15 officials said that generally they viewed 2016 as a success story because the attempted infiltration never got past the state's four layers of security.		
	DHS reported broad GRU scanning activity on State 15 government domains. 126		
State 16	(U) According to State 16 officials, cyber actors using infrastructure identified in the October FLASH conducted scanning activity against a state government network. ¹²⁷		
	DHS reported information on GRU scanning activity based on a self- report from State 16 after the issuance of the October FLASH. 128		
State 17	(U) State 17 officials reported nothing "irregular, inconsistent, or suspicious" leading up to the election. While State 17 fT staff received an MS-ISAC notification, that notification was not shared within the state government. DHS reported GRU scanning activity on an election-related domain.		
State 18	(U) State 18 election officials said they observed no connection from the IP addresses listed in the election-related notifications. 132		
	DHS reported indications of GRU scanning activity on a State 18 government domain. 133		
State 19	(U) According to State 19 officials, cyber actors using infrastructure identified in October by MS-ISAC conducted scanning activity. State 19 claimed this activity was "blocked," but did not elaborate on why or how it was blocked. 134		

¹²⁴ (UI) DHS IIR 4 019 0012 17, Cyber Activity Targeting [State 14] Government Networks from Internet Protocol Addresses Associated with Targeting State Elections Systems, October 21, 2016.

^{125 (}U) Memorandum for the Record, SSCI Staff, Conference Call with [State 15], March 12, 2018.

^{126 (}U) DHS briefing for Committee staff on March 5, 2018.

^{127 (}U) Memorandum for the Record, SSCI Staff, Conference Call with [State 16], December 1, 2017.

¹²⁸ (U) DHS briefing for Committee staff on March 5, 2018.

¹²th (U) Memorandum for the Record, SSCI Staff, Conference Call with [State 17], January 25, 2018.

^{(1) 1}bid.

⁽U) DHS briefing for Committee staff on March 5, 2018.

⁽U) Memorandum for the Record, SSCI Staff, Conference Call with [State 18], December 8, 2017.

⁽U) DHS briefing for Committee staff on March 5, 2018.

^{114 (}U) Memorandum for the Record, SSCI Staff, Conference Call with [State 19], December 1, 2017.

	DHS reported indications of GRU scanning activity on two separate State 19 government domains. 135
State 20	(U) According to State 20 officials, cyber actors using infrastructure identified in October by MS-ISAC were "knocking" on the state's network, but no successful intrusion occurred. 136
	DHS reported GRU scanning activity on the Secretary of State domain. 137
State 21	(U) State 21 officials received indicators from MS-ISAC in October 2016. They said they were not aware the state was among those targeted until notified. 138
State 21	DHS reported GRU scanning activity on an election-related domain as well as at least one other government system connected to the voter registration system. [39]

Neither DHS nor the Committee can ascertain a pattern to the states targeted, lending credence to DHS's later assessment that all 50 states probably were scanned. DHS representatives told the Committee that "there wasn't a clear red state-blue state-purple state, more electoral votes, less electoral votes" pattern to the attacks. DHS acknowledged that the U.S. Government does not have perfect insight, and it is possible the IC missed some activity or that states did not notice intrusion attempts or report them. 140



¹³⁵ (U) DHS briefing for Committee staff on March 5, 2018.

⁽U) Memorandum for the Record, SSCI Staff, Conference Call with [State 20], November 17, 2017.

⁽U) DHS briefing for Committee staff on March 5, 2018.

^{138 (}U) Memorandum for the Record, SSCI Staff, Conference Call with [State 21], November 17, 2017.

^{139 (}U) DHS briefing for Committee staff on March 5, 2018.

⁽U) SSCI interview with DHS and CTIIC, February 27, 2018, p. 25.

⁽U) SSCI interview with DHS and CTIIC, February 27, 2018, p. 21.

(U) As of October 2018, the IC and DHS were looking for evidence of threats to election systems,

An October 11, 2018 DHS Intelligence Assessment reported the following:

We judge that numerous actors are regularly targeting election infrastructure, likely for different purposes, including to cause disruptive effects, steal sensitive data, and undermine confidence in the election. We are aware of a growing volume of malicious activity targeting election infrastructure in 2018, although we do not have a complete baseline of prior years to determine relative scale of the activity. Much of our understanding of cyber threats to election infrastructure is due to proactive sharing by state and local election officials, as well as more robust intelligence and information sharing relationships amongst the election community and within the Department. The observed activity has leveraged common tactics—the types of tactics that are available to nation-state and non-state cyber actors, alike—with limited success in compromising networks and accounts. We have not attributed the activity to any foreign adversaries, and we continue to work to identify the actors behind these operations. At this time, all these activities were either prevented or have been mitigated.

(U// Specifically:

Unidentified cyber actors since at least April 2018 and as recently as early October continue to engage in a range of potential elections-related cyber incidents targeting election infrastructure using spear-phishing, database exploitation techniques, and denial of service attacks, possibly indicating continued interest in compromising the availability, confidentiality, and integrity of these systems. For example, on 24 August 2018, cybersecurity officials detected multiple attempts to illegally access the State of Vermont's Online Voter Registration Application (OLVR), which serves as the state's resident voter registration database, according to DHS reporting. The malicious activity included one Cross Site Scripting attempt, seven Structured Query Language (SQL) injection attempts, and one attempted Denial of Service (DoS) attack. All attempts were unsuccessful. 143

(U//) In summarizing the ongoing threat to U.S. election systems, DHS further said in the same product, "We continue to assess multiple elements of U.S. election infrastructure are potentially vulnerable to cyber intrusions." 144

B. (U) Russian Access to Election Infrastructure

⁽Uh) DHS, Homeland Security Intelligence Assessment, Cyber Actors Continue to Engage in Influence Activities and Targeting of Election Infrastructure, October 11, 2018.
144 (U) Ibid.

(U) The January 6, 2017 Intelligence Community Assessment (ICA), "Assessing Russian Activities and Intentions in Recent U.S. Elections," states:

Russian intelligence obtained and maintained access to elements of multiple U.S. state or local electoral boards. DHS assesses that the types of systems Russian actors targeted or compromised were not involved in vote tallying. 145

Based on the Committee's review of the ICA, the Committee concurs with this assessment. The Committee found that Russian-affiliated cyber actors gained access to election infrastructure systems across two states, including successful extraction of voter data. However, none of these systems were involved in vote tallying.

1. (U) Russian Access to Election Infrastructure: Illinois

- (U) In June 2016, Illinois experienced the first known breach by Russian actors of state election infrastructure during the 2016 election. As of the end of 2018, the Russian eyber actors had successfully penetrated Illinois's voter registration database, viewed multiple database tables, and accessed up to 200,000 voter registration records. The compromise resulted in the exfiltration of an unknown quantity of voter registration data. Russian eyber actors were in a position to delete or change voter data, but the Committee is not aware of any evidence that they did so. 149
 - DHS assesses with high confidence that the penetration was carried out by Russian actors. 150
 - (U/ ______) The compromised voter registration database held records relating to 14 million registered voters, _______. The records exfiltrated included information on each voter's name, address, partial social security number, date of birth, and either a driver's license number or state identification number. ¹⁵¹

SCI Open Hearing on June 21, 2017, p 110

(City) I BI IIK

DHS Intelligence Assessment, May 3, 2017, 0144-17.

p. 2.

⁽ii) Intelligence Community Assessment, Assessing Russian Activities and Intentions in Recent U.S. Elections, January 6, 2017, p. iii.

⁽U) DHS IIR 4 005 0006, An IP Address Targeted Multiple U.S. State Government's to Include Election Systems, October 4, 2016; DHS briefing for SSCI staff, March 5, 2018.

^{(4) &}quot;Illinois election officials say hack yielded information on 200,000 voters," [Local Newspaper], August 29, 2016.

^{148 (}U) DHS IIR

⁽U) State Board of Elections, Illinois Voter Registration System Records Breached, August 31, 2016. As reflected elsewhere in this report, the Committee did not undertake its own forensic analysis of the Illinois server logs to corroborate this statement; SSCI interview with DHS and CTIIC, February 27, 2018, p. 24.

^{150 (}U) See Infra, "Russian Scanning and Attempted Access to Election-Related Infrastructure" for a complete discussion on attribution related to the set of cyber activity linked to the infrastructure used in the Illinois breach.
151 (UII) FBI IIR

- DHS staff further recounted to the Committee that "Russia would have had the ability to potentially manipulate some of that data, but we didn't see that." ¹⁵² Further, DHS staff noted that "the level of access that they gained, they almost certainly could have done more. Why they didn't . . . is sort of an open-ended question. I think it fits under the larger umbrella of undermining confidence in the election by tipping their hand that they had this level of access or showing that they were capable of getting it." ¹⁵³
- (U) According to a Cyber Threat Intelligence Integration Center (CTIIC) product, Illinois officials "disclosed that the database has been targeted frequently by hackers, but this was the first instance known to state officials of success in accessing it." 154
- (U) In June 2017, the Executive Director of the Illinois State Board of Elections (SBE), Steve Sandvoss, testified before the Committee about Illinois's experience in the 2016 elections. ¹⁵⁵ He laid out the following timeline:
 - (U) On June 23, 2016, a foreign actor successfully penetrated Illinois's databases through an SQL attack on the online voter registration website. "Because of the initial low-volume nature of the attack, the State Board of Election staff did not become aware of it at first." 156
 - (U) Three weeks later, on July 12, 2016, the IT staff discovered spikes in data flow
 across the voter registration database server. "Analysis of the server logs revealed that
 the heavy load was a result of rapidly repeated database queries on the application status
 page of our paperless online voter application website." 157
 - (U) On July 13, 2016, IT staff took the website and database offline, but continued to see activity from the malicious IP address. 158
 - (U) "Firewall monitoring indicated that the attackers were hitting SBE IP addresses five times per second, 24 hours a day. These attacks continued until August 12th [2016], when they abruptly ceased." 159

154 (U) CTIIC Cyber Threat Intelligence Summary, August 18, 2016.

^{152 (}U) SSCI interview with DHS and CTIIC, February 27, 2018, p. 14.

^{153 (}U) Ibid.

^{155 (}U) SSCI Open Hearing on June 21, 2017. The Committee notes that, in his testimony, Mr. Sandvoss said Illinois still had not been definitively told that Russia perpetrated the attack, despite DHS's high confidence. The Committee also notes that DHS eventually provided a briefing to states during which DHS provided further information on this topic, including the DHS high-confidence attribution to Russia.

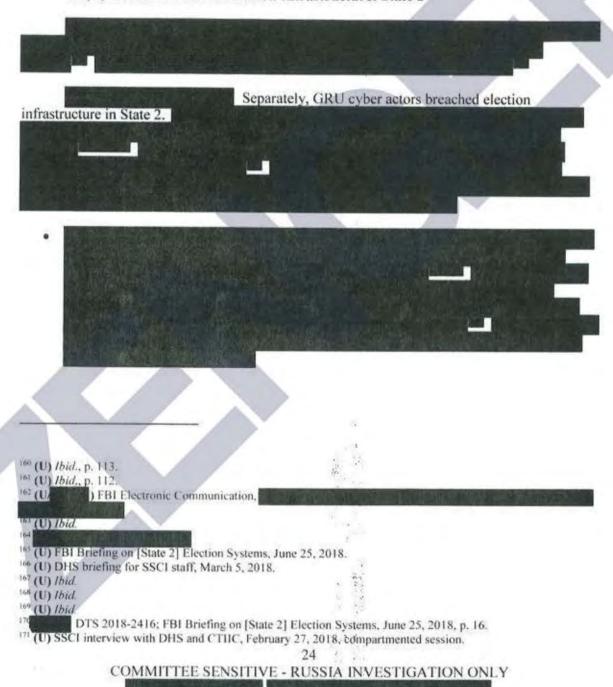
^{156 (}U) Ibid., p. 110.

^{157 (}U) Ibid.

^{158 (}U) Ibid., p. 111.

^{159 (}U) Ibid.

- (U) On July 19, 2016, the election staff notified the Illinois General Assembly and the Attorney General's office.
- (U) Approximately a week later, the FBI contacted Illinois. 160
- (U) On July 28, 2016, both the registration system and the online voter registration became fully functional again. ¹⁶¹
 - 2. (U) Russian Access to Election Infrastructure: State 2



		_	
•			

	(U) FBI and DHS Interactions with State 2179		
August 18, 2016	(U) FBI FLASH notification identified IP addresses targeting election offices. 180		
August 24, 2016	(U) State 2 Department of State received the FLASH from National Association of Secretaries of State. [18]		
August 26, 2016	(U) State 2 Department of State forwarded FLASH to counties and advised them to block the IP addresses. 182		
	Separately, determined one of the listed IP addresses scanned its system. 183 subsequently discovered suspected intrusion activity and contacted the FBI. 184		

^{172 (}U) Ibid.

25

^{123 (}U) Ibid.

^{174 (}U) Ibid.

DTS 2018-2416; FBI Briefing on [State 2] Election Systems, June 25, 2018, pp. 7.

^{176 (}U) Ibid.

¹⁹⁷ Ibid. See also EB-0004893-LED

⁽U) SSCI interview with DHS and CTIIC, February 27, 2018, p. 42.

DTS 2018-2416; FBI Briefing on [State 2] Election Systems, June 25, 2018, pp. 7.

^{180 (}U) FBI FLASH, Alert Number T-LD1004-TT, TLP-AMBER,

DTS 2018-2416; FBI Briefing on [State 2] Election Systems, June 25, 2018, p. 4.

^{182 (}U) Ibid., pp. 4-5.

^{183 (}U) Ibid., p. 5.

^{184 (}U) Ibid.

August 31, 2016	FBI opened its investigation on the and "conducted outreach to State 2 county election officials to discuss individual security postures and any suspicious activity." [185] FBI outreach reveals that one State 2 county—County A—was scanned. [186]
September 30, 2016	FBI held a conference call with county election officials to advise of the attempt to probe County A. FBI also notified state and local officials of available DHS services. F88
October 4, 2016	County B's IT administrator contacted FBI regarding a potential intrusion. 189 According to the FBI, "Of particular concern, the activity included a connection to a county voting, testing, and maintenance server used for poll worker classes." 190
October 14, 2016	(U) FBI shared County B indicators by issuing a FLASH. 1917
December 29, 2016	(U) DHS and FBI released a Joint Analysis Report (JAR) on the "GRIZZLY STEPPE" intrusion set; report represents the first IC attribution of state election-related systems to the Russians. 192
June 2017	(U) DHS notified State 2 counties of a possible intrusion "as part of a broader notification to 122 entities identified as spearphishing victims in an intelligence report." 194

194 (U) Ibid.

DTS 2018-2416; FBI Briefing on [State 2] Election Systems, June 25, 2018, p. 5.

^{186 (}U) Ibid.

^{187 (}U) Ibid., pp. 5-6.

^{188 (}U) Ibid., p. 6.

^{189 (}U) Ibid.

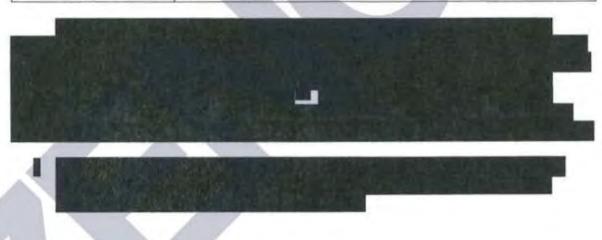
^{190 (}U) Ibid.

⁾ FBI FLASH, Alert Number T-LD1005-TT, TLP-AMBER,

¹⁹³ (U) DHS/FBI, Joint Analysis Report, JAR-16-20296A, GRIZZLY STEPPE – Russian Malicious Cyber Activity, December 29, 2016.

DTS 2018-2416; FBI Briefing on [State 2] Election Systems, June 25, 2018, p. 7.

July 2017	(U) FBI published a FLASH report warning of possible spearphishing. 195
November 2017	(U) FBI and DHS participated in the first meeting of the State 2 elections task force. 196
February 2018	(U) FBI requested direct engagement with Counties B, C, and D, including a reminder of available DHS services. 197
March 2018	(U) FBI reports that "our office engaged" the affected counties through the local FBI field office. 198 The FBI could not provide any further detail on the substance of these engagements to the Committee.
May 29, 2018	*FBI provided a SECRET Letterhead Memo to DHS "formally advising of our investigation into the intrusion , the reported intrusion at County B, and suspected compromises of Counties C and D.**199
June 11, 2018	(U) FBI reports that as of June 11, 2018, Counties A, B, C, and I had not accepted DHS services. 200



105 (U) FBI FLASH, Alert Number EB-000083-LD, TLP-AMBER,

. See DTS 2018-3174.

27

DTS 2018-2416; FBI Briefing on [State 2] Election Systems, June 25, 2018, p. 7.

^{197 (}U) Ibid., p. 6.

^{198 (}U) Ibid., p. 34.

^{199 (}U) Ibid., pp. 8-9.

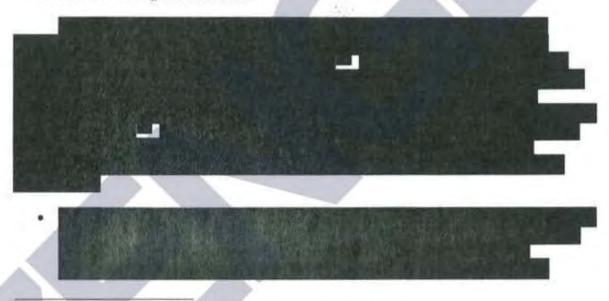
^{200 (}U) Ibid. p. 20.

DTS 2018-2416; FB1 Briefing on [State 2] Election Systems, June 25, 2018, pp. 20-21.

DHS briefing for SSCI staff, March 5, 2018.

- (U) State 2's Secretary of State and Election Director told the Committee in December 2017 that there was "never an attack on our systems." "We did not see any unusual activities. I would have known about it personally." State 2 did not want to share with the Committee its cybersecurity posture, but state officials communicated that they are highly confident in the security of their systems.
- (U) State 2's election apparatus is highly decentralized, with each county making its own decisions about acquiring, configuring, and operating election systems.²⁰⁸
- (U) As of August 9, 2018, DHS was complimentary of the steps State 2 had taken to secure its voting systems, including putting nearly all counties on the ALBERT sensor system, joining the Elections Infrastructure Information Sharing and Analysis Center (El-ISAC), and using congressionally appropriated funds plus additional state funds to hire cybersecurity advisors.²⁰⁶

C. (U) Russian Efforts to Research U.S. Voting Systems, Processes, and Other Elements of Voting Infrastructure



^{283 (}U) Memorandom for the Record, SSCI Staff, Conference Call with [State 2], December 1, 2017.

^{201 (}U) Ibid.

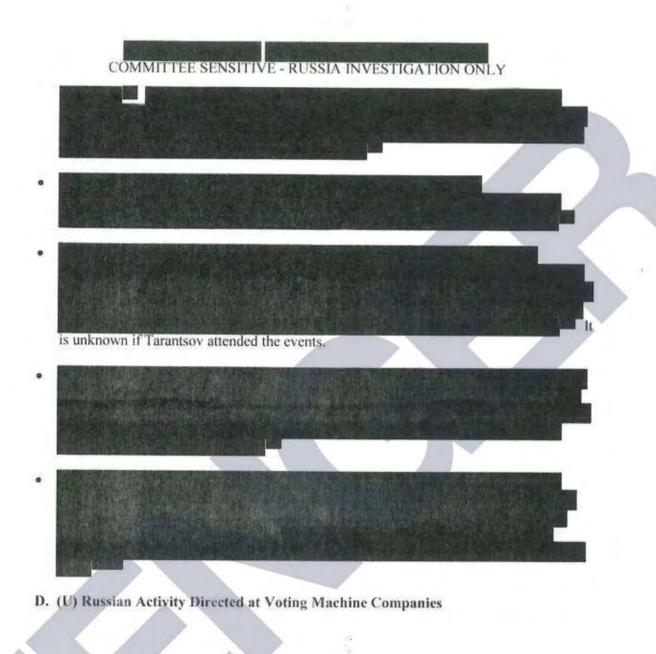
^{205 (}U) Ibid.

⁽U) DTS 2018-2581, Memorandum for the Record, Telephone call with DHS, August 9, 2018.

FBI LHM,

⁽U) Ibid., p. 5.

Note: "FISA" refers to electronic surveillance collected on a foreign power or an agent of a foreign power pursuant to the Foreign Intelligence Surveillance Act of 1978. This collection could have come from landlines, electronic mail accounts, or mobile phones used by personnel at a foreign embassy (i.e., an "establishment" FISA) or used by personnel associated with a foreign power (i.e., "agents of a foreign power"). This FISA collection would have been approved by the Foreign Intelligence Surveillance Court ("FISC"), effectuated by FBI, and then could also have been shared with NSA or CIA, or both, depending on the foreign target.





COMMITTEE SENSITIVE - RUSSIA INVESTIGATION ONLY Russian government actors engaged in

attacks on

FBI reported that "between December 2015 and June 2016,

DHS further told the Committee that malicious cyber actors had scanned of election systems, 219

E. (U) Russian Efforts to Observe Polling Places

election systems,

Department of State were aware that Russia was attempting to send election observers to polling places in 2016. The true intention of these efforts is unknown.

EBI Electronic Communication,

219 (U) DHS briefing for SSCI staff, March 5, 2018.

221 (U) Ibid.

222 (U) Ibid.

223 (U) NSA DIRNSA, May 5, 2017, p. 3.

224 (U) Ibid., pp. 1-3.

225 (U) FBI IIR

226 (U) Ibid.

The Russian Embassy placed a formal request to observe the elections with the Department of State, but also reached outside diplomatic channels in an attempt to secure permission directly from state and local election officials.227 For example, in September 2016, the State 5 Secretary of State denied a request by the Russian Consul General to allow a Russian government official inside a polling station on Election Day to study the U.S. election process, according to State 5 officials. 228 n mission." nterfere

```
227 (U) DTS 2018-2152, SSCT Transcript of the Interview of Andrew McCabe, Former Deputy Director of the Federal Bureau of Investigation, February 14, 2018, pp. 221-222.

228 (U) Ibid.
230 (U) Ibid.
231 Email, sent November 4, 2016; from to:

232 Email, sent: September 13, 2016; from:

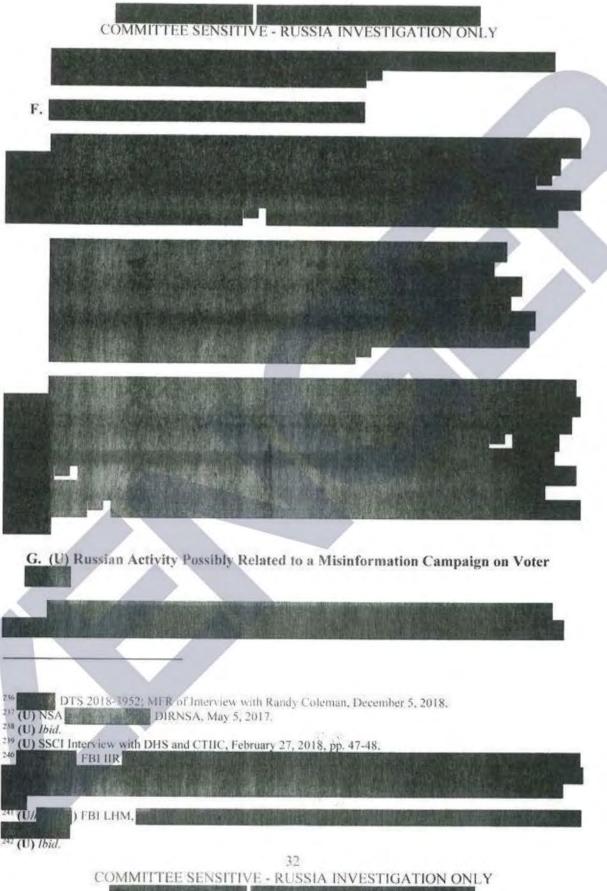
233 (U) Ibid.
234 (U) Ibid.
235 Email Sent: Monday, November 7, 2016, 8:11 AM; from:

236 Email Sent: Monday, November 7, 2016, 8:11 AM; from:

237 Email Sent: Monday, November 7, 2016, 8:11 AM; from:

238 Email Sent: Monday, November 7, 2016, 8:11 AM; from:

249 Email Sent: Monday, November 7, 2016, 8:11 AM; from:
```

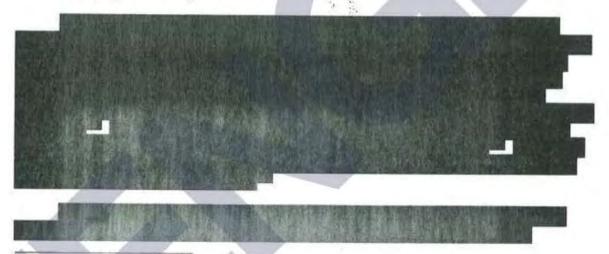




- (U) The declassified, January 6, 2017, Intelligence Community Assessment also highlighted preparations related to voter fraud, noting that Russian diplomats "were prepared to publicly call into question the validity of the results" and that "pro-Kremfin bloggers had prepared a Twitter campaign, #DemocracyRIP, on election night in anticipation of Secretary Clinton's victory, judging from their social media activity."²⁴⁵
- (U) During a 2017 election, State 17 saw bot activity on social media, including allegations of voter fraud, in particular on Reddit. State 17 had to try to prove later that there was no fraud.²⁴⁶

H. (U) Two Unexplained Events

I. (U) Cyber Activity in State 22



²⁴⁸

⁽U) Intelligence Community Assessment, Assessing Russian Activities and Intentions in Recent U.S. Elections, January 6, 2017, p. 2.

²⁴⁶ (U) See Memorandum for the Record, SSCI Staff, Conference Call with State 17, January 25, 2018. The Committee notes it is conducting a related investigation into the use of social media by Russian-government affiliated entities.

²⁴⁷ (U) The Fusion Center model is a partnership between DHS and state, local, tribal, and territorial entities. They serve as a focal point for "the receipt, analysis, gathering, and sharing of threat-related information."

²⁴⁸ (U) CTHC Cyber Threat Intelligence Summary/Cyber Threats in Focus, Malicious Cyber Activity on Election-Related Computer Networks Last Spring Possibly Linked to Russia, October 7, 2016; DHS, HR 4 019 0147 16, September 28, 2016.

^{249 (}U) Ibid

^{250 (}U) Ibid

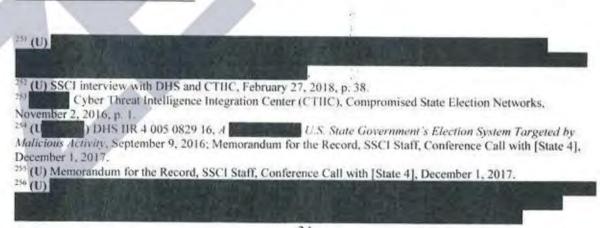
2. (U) Cyber Activity in State 4

(Umber 1) State 4 officials, DHS, and FBI in the spring and summer of 2016, struggled to understand who was responsible for two rounds of cyber activity related to election infrastructure. Eventually, one set of cyber activity was attributed to Russia and one was not.

(Umage) First, in April of 2016, a cyber actor successfully targeted State 4 with a phishing scam. After a county employee opened an infected email attachment, the cyber actor stole credentials, which were later posted online. Those stolen credentials were used in June 2016 to penetrate State 4's voter registration database. A CTHC product reported the incident as follows: An unknown actor viewed a statewide voter registration database after obtaining a state employee's credentials through phishing and keystroke logging malware, according to a private-sector DHS partner claiming secondhand access. The actor used the credentials to access the database and was in a position to modify county, but not statewide, data." 253

(U) DHS analysis of forensic data provided by a private sector partner discovered malware on the system, and State 4 shut down the voter registration system for about eight days to contain the attack. 254 State 4 officials later told the Committee that that while the cyber actor was able to successfully log in to a workstation connected to election related infrastructure, additional credentials would have been needed for the cyber actor to access the voter registration database on that system. 255

(U) At first, FBI told State 4 officials that the attack may have originated from Russia, but the ties to the Russian government were unclear. "The Bureau described the threat as 'credible' and significant, a spokesman for State 4 Secretary of State said." State 4 officials also told press that the hacker had used a server in Russia, but that the FBI could not confirm the



34

attack was tied to the Russian government.²⁵⁷ DHS and FBI later assessed it to be criminal activity, with no definitive tie to the Russian government.²⁵⁸

Subsequently, Russian actors engaged in the same scanning activity as seen in other states, but directed at a domain affiliated with a public library. 259 Officials saw no effective penetration of the system. DHS has low confidence that this cyber activity is attributable to the Russian intelligence services because the target was unusual and not directly involved in elections. 260

V. (U) RUSSIAN INTENTIONS

- (U) Russian intentions regarding U.S. election infrastructure remain unclear. Russia might have intended to exploit vulnerabilities in election infrastructure during the 2016 elections and, for unknown reasons, decided not to execute those options. Alternatively, Russia might have sought to gather information in the conduct of traditional espionage activities. Lastly, Russia might have used its activity in 2016 to catalog options or clandestine actions, holding them for use at a later date. Based on what the IC knows about Russia's operating procedures and intentions more broadly, the IC assesses that Russia's activities against U.S. election infrastructure likely sought to further their overarching goal: undermining the integrity of elections and American confidence in democracy.
 - (U) Former-Homeland Security Adviser Lisa Monaco told the Committee that "[t]here
 was agreement [in the IC] that one of the motives that Russia was trying to do with this
 active measures campaign was to sow distrust and discord and lack of confidence in the
 voting process and the democratic process." 262
 - DHS representatives told the Committee that "[w]e see . . . Russians in particular obviously, gain access, learn about the environment, learn about what systems are interconnected, probing, the type of intelligence preparation of the environment that you would expect from an actor like the Russians. So certainly the context going forward

258 (U) SSCI interview with DHS and CTIIC, February 27, 2018, p. 40.
259 (U)

DHS/FBI Homeland Intelligence Brief,

261 (U) Ibid.
262 (ID SSCI Transgript of the Interview with of Lies Manage Former Homeland Formity Advisor Asset 10

²⁶² (U) SSCI Transcript of the Interview with of Lisa Monaco, Former Homeland Security Advisor, August 10, 2017, p. 30.

is a concern of what they might have learned and how much more they know about the systems."263

- Mr. McCabe told the Committee that it seemed to him like "classic Russian cyber espionage. . . . [They will] scrape up all the information and the experience they possibly can," and "they might not be effective the first time or the fifth time, but they are going to keep at it until they can come back and do it in an effective way." 264
- Mr. Daniel told the Committee:

While any one voting machine is fairly vulnerable, as has been demonstrated over and over again publicly, the ability to actually do an operation to change the outcome of an election on the scale you would need to, and do it surreptitiously, is incredibly difficult. A much more achievable goal would be to undermine confidence in the results of the electoral process, and that could be done much more effectively and easily. . . . A logical thing would be, if your goal is to undermine confidence in the U.S. electoral system which the Russians have a long goal of wanting to put themselves on the same moral plane as the United States . . . one way would be to cause chaos on election day. How could you start to do that? Mess with the voter registration databases. 265

Ms. Monaco further echoed that concern:

Well, one of the things I was worried about—and I wasn't alone in this—is kind of worst-case scenarios, which would be things like the voter registration databases. So if you're a state and local entity and your voter registration database is housed in the secretary of state's office and it is not encrypted and it's not backed up, and it says Lisa Monaco lives at Smith Street and I show up at my [polling place] and they say 'Well we don't have Ms. Monaco at Smith Street, we have her at Green Street,' now there's difficulty in my voting. And if that were to happen on a large scale, I was worried about confusion at polling places, lack of confidence in the voting system, anger at a large scale in some areas, confusion, distrust. So there was a whole sliding scale of

^{263 (}U) SSCI interview with DHS and CTHC, February 27, 2018, p. 15.

²⁶⁴ (U) DTS 2018-2152, SSCI Transcript of the Interview with Andrew McCabe, Former Deputy Director of the FBI, February 14, 2018, pp. 224-225.

²⁶⁵ (U) SSC1 Transcript of the Interview with Michael Daniel, Former Assistant to the President and Cybersecurity Coordinator, National Security Council, August 31, 2017, pp. 27, 34.

horribles just when you're talking about voter registration databases. 266



(U) Chaos on Election Day: Three Scenarios

Mr. Daniel said that in the early fall of 2016, a policy working group was looking at three scenarios:

One was, could the Russians do something to the voter registration databases that could cause problems on Election Day? An example of that would be, could you go in and flip the digits in everybody's address, so that when they show up with their photo ID it doesn't match what's in the poll book? It doesn't actually prevent people from voting. In most cases you'll still get a provisional ballot, but if this is happening in a whole bunch of precincts for just about everybody showing up, it gives the impression that there's chaos. 268

A second one was to do a variant of the penetrating voting machines, except this time what you do is you do a nice video of somebody conducting a hack on a voting machine and showing how you could do that hack and showing them changing a voting outcome, and then you post that on YouTube and you claim you've done this 100,000 times across the United States, even though you haven't actually done it at all. 269

Then the third scenario that we looked at was conducting a denial of service attack on the Associated Press on Election Day, because pretty much everybody, all those nice maps that everybody puts up on all the different news services, is in fact actually based on Associated Press stringers at all the different precincts and locations. . . . It doesn't actually change anything, but it gives the impression that there's chaos. 270

270 (U) Ibid., p. 35.

²⁶⁶ (U) SSCI Transcript of the Interview with Lisa Monaco, Former Homeland Security Advisor, August 10, 2017, p. 28.

²⁶⁸ (U) SSCI Transcript of the Interview with Michael Daniel, Former Assistant to the President and Cybersecurity Coordinator, National Security Council, August 31, 2017, p. 33.
²⁶⁹ (U) *Ibid.*, pp. 34-35.



VI. (U) NO EVIDENCE OF CHANGED VOTES OR MANIPULATED VOTE TALLIES

- (U) In its review, the Committee has seen no indications that votes were changed, votetallying systems were manipulated, or that any voter registration data was altered or deleted,
 although the Committee and IC's insight is limited. Poll workers and voting monitors did not
 report widespread suspicious activity surrounding the 2016 election. DHS Assistant Secretary
 Jeanette Manfra said in the Committee's open hearing in June 2017 that "I want to reiterate that
 we do have confidence in the overall integrity of our electoral system because our voting
 infrastructure is fundamentally resilient." Further, all three witnesses in that hearing—Ms.
 Manfra, Dr. Liles, and FBI Assistant Director for Counterintelligence Bill Priestap—agreed that
 they had no evidence that votes themselves were changed in any way in the 2016 election. 271
 - (U) Dr. Liles said that DHS "assessed that multiple checks and redundancies in U.S. election infrastructure, including diversity of systems, non-internet connected voting machines, pre-election testing and processes for media, campaign and election officials to check, audit, and validate the results—all these made it likely that cyber manipulation of the U.S. election systems intended to change the outcome of the national election would be detected."
 He later said "the level of effort and scale required to change the outcome of a national election would make it nearly impossible to avoid detection."

 - (U) States did not report either an uptick in voters showing up at the polls and being unable to vote or a larger than normal quantity of provisional ballots.
- (U) The Committee notes that nationwide elections are often won or lost in a small number of precincts. A sophisticated actor could target efforts at districts where margins are already small, and disenfranchising only a small percentage of voters could have a disproportionate impact on an election's outcome.
- (U) Many state election officials emphasized their concern that press coverage of, and increased attention to, election security could create the very impression the Russians were seeking to foster, namely undermining voters' confidence in election integrity. Several insisted that whenever any official speaks publicly on this issue, they should state clearly the difference between a "scan" and a "hack," and a few even went as far as to suggest that U.S. officials stop

271 (U) Ibid., p. 47.

²⁷¹ (U) SSC1 Transcript of the Open Hearing on Russian Interference in the 2016 U.S. Elections, held on Wednesday, June 21, 2017.

²⁷² (U) SSC1 Transcript of the Open Hearing on Russian Interference in the 2016 U.S. Elections, held on Wednesday, June 21, 2017, p. 13.

talking about the issue altogether. One state official said, "We need to walk a fine line between being forthcoming to the public and protecting voter confidence." 274

(U) Mr. Brennan described a similar concern in IC and policy discussions:

We know that the Russians had already touched some of the electoral systems, and we know that they have capable cyber capabilities. So there was a real dilemma, even a comundrum, in terms of what do you do that's going to try to stave off worse action on the part of the Russians, and what do you do that is going to . . . [give] the Russians what they were seeking, which was to really raise the specter that the election was not going to be fair and unaffected.²⁷⁵

- (U) Most state representatives interviewed by the Committee were confident that they met the threat effectively in 2016 and believed that they would continue to defeat threats in 2018 and 2020. Many had interpreted the events of 2016 as a success story: firewalls deflected the hostile activity, as they were supposed to, so the threat was not an issue. One state official told the Committee, "I'm quite confident our state security systems are pretty sound." Another state official stated, "We felt good [in 2016]," and that due to additional security upgrades, "we feel even better today." 277
- (U) However, as of 2018, some states were still grappling with the severity of the threat. One official highlighted the stark contrast they experienced, when, at one moment, they thought elections were secure, but then suddenly were hearing about the threat. The official went on to conclude, I don't think any of us expected to be backed by a foreign government. Another official, paraphrasing a former governor, said, If a nation-state is on the other side, it's not a fair fight. You have to phone a friend.
- (U) In the month before Election Day, DHS and other policymakers were planning for the worst-case scenario of efforts to disrupt the vote itself. Federal, state, and local governments created incident response plans to react to possible confusion at the polling places. Mr. Daniel said of the effort: "We're most concerned about the Russians, but obviously we are also concerned about the possibility for just plain old hacktivism on Election Day.... The incident response plan is actually designed... to help us [plan for] what is the federal government going to do if bad things start to happen on Election Day?"

Mr. Daniel added that this was the first opportunity to exercise the process established under Presidential Policy Directive-41. "We asked the various agencies with lead

⁽U) Memorandum for the Record, SSCI Staff, Conference Call with [State 8], February 2, 2018.

^{278 (}U) SSCI Transcript of the Interview with John Brennan, Former Director, CIA, held on Friday, June 23, 2017, p. 54

²⁷⁶ (U) Memorandum for the Record, SSCI Staff, Conference Call with [State 6], November 17, 2017.

²⁷⁷ (U) Memorandum for the Record, SSCI Staff, Conference Call with [State 8], February 2, 2018.

²⁷⁸ (U) Memorandum for the Record, SSCI Staff, Conference Call with [State 20], November 17, 2017.

^{279 (}U) Ibid.

²⁸⁰ (U) Memorandum for the Record, SSCI Staff, Conference Call with [State 9], November 17, 2017.

responsibility, all right, give us your Election Day plan." That led to the creation of an Election Day playbook; steps included enhanced watch floor procedures, connectivity between FBI field offices and FBI and DHS, and an "escalation path" if "we needed to get to Lisa [Monaco] or Susan [Rice] in a hurry" on Election Day. 281

VII. (U) SECURITY OF VOTING MACHINES

- (U) The Committee review of Russian activity in 2016 highlighted potential vulnerabilities in many voting machines, with previous studies by security researchers taking on new urgency and receiving new scrutiny. Although researchers have repeatedly demonstrated it is possible to exploit vulnerabilities in electronic voting machines to alter votes,²⁸² some election officials dispute whether such attacks would be feasible in the context of an actual election.
 - (U) Dr. Alex Halderman, Professor of Computer Science at the University of Michigan, testified before the Committee in June 2017 that "our highly computerized election infrastructure is vulnerable to sabotage and even to cyber attacks that could change votes." ²⁸³ Dr. Halderman concluded, "Voting machines are not as distant from the internet as they may seem." ²⁸⁴
 - (U) When State 7 decommissioned its Direct-Recording Electronic (DRE) voting machines in 2017, the IT director led an exercise in attempting to break into a few of the machines using the access a "normal" voter would have in using the machines. ²⁸⁵ The results were alarming: the programmed password on some of the machines was ABC123, and the testers were able to flip the machines to supervisor mode, disable them, and "do enough damage to call the results into question." ²⁸⁶ The IT director shared the results with State 21 and State 24, which were using similiar machines. ²⁸⁷
 - (U) In 2017, DEFCON²⁸⁸ researchers were able to find and exploit vulnerabilities in five different electronic voting machines.²⁸⁹ The WinVote machines, those recently decertified by State 7, were most easily manipulated. One attendee said, "It just took us a couple of hours on Google to find passwords that let us unlock the administrative

282 (U) See also, Infra, "Direct-Recording Electronic (DRE) Voting Machine Vulnerabilities."

^{281 (}U) Ibid., p. 82.

²⁸¹ (U) SSCI Transcript of the Open Hearing on Russian Interference in the 2016 U.S. Elections, held on Wednesday, June 21, 2017, p. 117.

^{284 (}U) Ibid., p. 110,

^{285 (}U) Memorandum for the Record, SSCI Staff, Conference Call with [State 7], January 25, 2018.

^{286 (}U) Ibid. The machines used were WinVote voting machines.

⁽U) Ibid.

^{288 (}U) DEFCON is an annual hacker conference held in Las Vegas, Nevada. In July 2017, at DEFCON 25, the conference featured a Voting Machine Hacking Village ("Voting Village") which acquired and made available to conference participants over 25 pieces of election equipment, including voting machines and electronic poll books, for generally unrestricted examination for vulnerabilities.

^{289 (}U) Matt Blaze, et. al., DEFCON 25: Voting Machine Hacking Village: Report on Cyber Vulnerabilities in U.S. Election Equipment, Databases, and Infrastructure, September 2017, https://www.defcon.org/images/defcon-25/DEF%20CON%2025%20voting%20report.pdf, pp. 8-13.

functions on this machine,"290 A researcher was able to hack into the WinVote over WiFi within minutes using a vulnerability from 2003. 291 Once he had administrator-level access, he could change votes in the database. Researchers also discovered available USB ports in the machine that would allow a hacker to run software on the machine. 292 One said "with physical access to back [sic] of the machine for 15 seconds, an attacker can do anything." Hackers were less successful with other types of machines, although each had recorded vulnerabilities. 294

- (U) The 2018 DEFCON report found similar vulnerabilities, in particular when hackers had physical access to the machines. For example, hackers exploited an old vulnerability on one machine, using either a removable device purchasable on eBay or remote access, to modify vote counts.²⁹⁵
- (U/S) DHS briefed the Committee in August 2018 that these results were in part because the hackers had extended physical access to the machines, which is not realistic for a true election system. Undersecretary Krebs also disagreed with reporting that a 17-year-old hacker had accessed voter tallies. Some election experts have called into question the DEFCON results for similar reasons and pointed out that any fraud requiring physical access would be, by necessity, small scale, unless a government were to deploy agents across thousands of localities.
- (U) ES&S Voting Systems disclosed that some of its equipment had a key security vulnerability. ES&S installed remote access software on machines it sold in the mid-2000s, which allowed the company to provide ΓΓ support more easily, but also created potential remote access into the machines. When pressed by Senator Ron Wyden of Oregon, the company admitted that around 300 voting jurisdictions had the software. ES&S says the software was not installed after 2007, and it was only installed on election-management systems, not voting machines.²⁹⁷ More than 50 percent of voters vote on ES&S equipment, and 41 states use its products.

²⁹⁰ (U) Elizabeth Wise, "Hackers at DefCon Conference Exploit Vulnerabilities in Voting Machines," USA Today, July 30, 2017, https://www.usatoday.com/story/tech/2017/07/30/hackers-defcon-conference-exploit-vulnerabilities-voting-machines/523639001/.

⁽U) Matt Blaze, et, al., DEFCON 25. Voting Machine Hacking Village: Report on Cyber Vulnerabilities in U.S. Election Equipment, Databases, and Infrastructure, September 2017, https://www.defcon.org/images/defcon-25/DEF%20CON%2025%20voting%20report.pdf, p. 4.

⁽U) Ibid., p. 9.

^{293 (}U) Ibid.

^{294 (}U) thid., pp. 8-13.

²⁹⁵ (U) Robert McMillian and Dustin Volz, "Voting Machine Used in Half of U.S. Is Vulnerable to Attack, Report Finds," Wall Street Journal, September 27, 2018. The machine referenced is the ES&S Model 650, which ES&S stopped making in 2008 but is still available for sale.

²⁹⁶ (U) DTS 2018-3275, Summary of 8/22/2018 All Senators Election Security Briefing, August 28, 2018
²⁹⁷ (U) Hacks, Security Gaps And Oligarchs: The Business of Voting Comes Under Scrutiny, Miles Parks, NPR, September 21, 2018.

(U) Advocates of electronic voting point out the flaws in paper ballots, like the potential for the introduction of fraudulent ballots or invalidated votes due to stains or extra marks. The Committee believes that any election system should be protected end-to-end, including against fraud.

(U) Direct-Recording Electronic (DRE) Voting Machine Vulnerabilities

(U) While best practices dictate that electronic voting machines not be connected to the internet, some machines are internet-enabled. In addition, each machine has to be programmed before Election Day, a procedure often done either by connecting the machine to a local network to download software or by using removable media, such as a thumb drive. These functions are often carried out by local officials or contractors. If the computers responsible for writing and distributing the program are compromised, so too could all voting machines receiving a compromised update. Further, machines can be programmed to show one result to the voter while recording a different result in the tabulation. Without a paper backup, a "recount" would use the same faulty software to re-tabulate the same results, because the primary records of the vote are stored in computer memory.²⁹⁸

(U) Dr. Halderman said in his June 2017 testimony before SSCI:

I know America's voting machines are vulnerable because my colleagues and I have hacked them repeatedly as part of a decade of research studying the technology that operates elections and learning how to make it stronger. We've created attacks that can spread from machine to machine, like a computer virus, and silently change election outcomes. We've studied touchscreen and optical scan systems, and in every single case we found ways for attackers to sabotage machines and to steal votes. These capabilities are certainly within reach for America's enemies.

Ten years ago, I was part of the first academic team to conduct a comprehensive security analysis of a DRE voting machine. We examined what was at the time the most widely used touch-screen DRE in the country and spent several months probing it for vulnerabilities. What we found was disturbing: we could reprogram the machine to invisibly cause any candidate to win. 299

COMMITTEE SENSITIVE - RUSSIA INVESTIGATION ONLY

^{208 (}U) "Some DREs also produce a printed record of the vote and show it briefly to the voter, using a mechanism called a voter-verifiable paper audit trail, or VVPAT. While VVPAT records provide a physical record of the vote that is a valuable safeguard against cyberattacks, research has shown that VVPAT records are difficult to accurately audit and that voters often fail to notice if the printed record doesn't match their votes. For these reasons, most election security experts favor optical scan paper ballots." Written Statement by J. Alex Halderman, June 21, 2017, citing S. Goggin and M. Byrne, "An Examination of the Auditability of Voter Verified Paper Audit Trail (VVPAT) Ballots," Proceedings of the 2007 USENIX/ACCURATE Electronic Voting Technology Workshop, August 2007; B. Campbell and M. Byrne, "Now do Voters Notice Review Screen Anomalies?" Proceedings of the 2009 USENIX/ACCURATE/IAVoSS Electronic Voting Technology Workshop, August 2009.
299 (U) The machine was the Diebold AccuVote TS, which was still used statewide in at least one state as of 2017.

Cybersecurity experts have studied a wide range of U.S. voting machines—including both DREs and optical scanners—and in every single case, they've found severe vulnerabilities that would allow attackers to sabotage machines and to alter votes. That's why there is overwhelming consensus in the cybersecurity and election integrity research communities that our elections are at risk. 300

(U) In speaking with the Committee, federal government officials revealed concerns about the security of voting machines and related infrastructure. Former Assistant Attorney General for National Security John Carlin told the Committee:

"I'm very concerned about . . . our actual voting apparatus, and the attendant structures around it, and the cooperation between some states and the federal government." Mr. Carlin further stated, "We've literally seen it already, so shame on us if we can't fix it heading into the next election cycles. And it's the assessment of every key intel professional, which I share, that Russia's going to do it again because they think this was successful. So we're in a bit of a race against time heading up to the two-year election. Some of the election machinery that's in place should not be." 302

- (U) Mr. McCabe echoed these concerns, and noted that, in the last months before the election, FBI identified holes in the security of election machines, saying "there's some potential there." 303
- (U) As of November 2016, five states were using exclusively DRE voting machines with no paper trail, according to open source information.³⁰⁴ An additional nine states used at least some DRE voting machines with no paper trail.³⁰⁵
 - (U) State 20 has 21-year-old DRE machines. While the state is in the process of replacing its entire voting system, including these machines, State 20 is aiming to have the updates ready for the 2020 elections.
 - (U) In State 21, 50 of 67 counties as of November 2017 used DRE voting machines. 306

⁵⁰⁰ (U) SSCI Transcript of the Open Hearing on Russian Interference in the 2016 U.S. Elections, held on Wednesday, June 21, 2017, pp. 116-117.

³⁰¹ (U) SSCI Transcript of the Interview with John Carlin, Former Assistant Attorney General for National Security, held on Monday, September 25, 2017, p. 86.

^{302 (}U) Ibid., pp. 86-87.

³⁰³ (U) DTS 2018-2152, SSCI Interview with Andrew McCabe, Former Deputy Director of the FBI, February 14, 2018, p. 221.

³⁰² (U) BallotPedia, Voting Methods and Equipment By State, https://ballotpedia.org/Voting_methods_and_equipment_by_state.
³⁰⁵ (U) Ibid.

^{306 (}U) Memorandum for the Record, SSCI Staff, Conference Call with [State 21]. November 17, 2017.

- (U) State 5 used paper-backed voting in only about half its machines and DRE voting machines without paper backup in the other half.³⁰⁷
- (U) Some states are moving to a hybrid model—an electronic voting machine with a paper backup, often in the form of a receipt that prints after the voter submits their vote. For example, State 12 uses some DREs, but all equipment is required to have a paper trail, and the paper ballot is the ballot of record. State 12 also conducts a mandatory state-wide audit. Similarly, State 13 uses some paper-based and some electronic machines, but all are required to have a paper trail.
- (U) The number of vendors selling voting machines is shrinking, raising concerns about a vulnerable supply chain. A hostile actor could compromise one or two manufacturers of components and have an outsized effect on the security of the overall system.
 - "My job," said Ms. Monaco when asked whether she was worried about voting machines themselves getting hacked, "was to worry about every parade of horribles. So I cannot tell you that that did not cross my mind. We were worried about who, how many makers. We were worried about the supply chain for the voting machines, who were the makers? . . . Turns out I think it's just Diebold—and have we given them a defensive briefing? So to answer your question, we were worried about it all."
 - Mr. McCabe pointed out that a small number of companies have "90%" of the market for voting machines in the U.S. Before the 2016 election, briefed a few of the companies on vulnerabilities, 312 but a more comprehensive campaign to educate vendors and their customers is warranted.

(U) Voluntary Voting System Guidelines

(U) Part of the voting reform implemented under The Help America Vote Act of 2002 was a requirement that the Election Assistance Commission create a set of specifications and requirements against which voting systems can be tested, called the Voluntary Voting System Guidelines (VVSG). The EAC adopted the first VVSG in December 2005. The EAC then tasked the Technical Guidelines Development Committee, chaired by the National Institute of Standards and Technology (NIST) and including members from NASED, with updating the guidelines. In March 2015, the EAC approved VVSG 1.1; in January 2016, the EAC adopted

^{[10] (}U) Memorandum for the Record, SSCI Staff, Conference Call with [State 5], December 1, 2017.

³⁰⁸ (U) Memorandum for the Record, SSCI Staff, Conference Call with [State 12], December 1, 2017.

^{109 (}U) Ibid.

²¹⁰ (U) Memorandum for the Record, SSCI Staff, Conference Call with [State 13], December 1, 2017.

^{311 (}U) SSCI Transcript of the Interview with Lisa Monaco, Former Homeland Security Advisor, held on Thursday, August 10, 2017, p. 31.

^{312 (}U) SSC1 Transcript of the Interview with Andy McCabe, Deputy Director of the FBI, held on Wednesday, February 14, 2018, pp. 220-221.

an implementation plan requiring that all new voting systems be tested against the VVSG 1.1 beginning in July 2017. VVSG 1.1 has since been succeeded by version 2.0, which was released for a 90-day public comment period on February 15, 2019. The EAC will compile the feedback for Commissioners to review shortly thereafter. VVSG 2.0 includes the following minimum security guidelines:

- (U) An error or fault in the voting system software or hardware cannot cause an undetectable change in election results. (9.1)
- (U) The voting system produces readily available records that provide the ability to
 check whether the election outcome is correct and, to the extent possible, identify the
 root cause of any irregularities. (9.2)
- (U) Voting system records are resilient in the presence of intentional forms of tampering and accidental errors. (9.3)
- (U) The voting system supports strong, configurable authentication mechanisms to verify the identities of authorized users and includes multi-factor authentication mechanisms for critical operations. (11.3)
- (U) The voting system prevents unauthorized access to or manipulation of configuration data, cast vote records, transmitted data, or audit records. (13.1)
- (U) The voting system limits its attack surface by reducing unnecessary code, data paths, physical ports, and by using other technical controls. (14.2)
- (U) The voting system employs mechanisms to protect against malware. (15.3)
- (U) A voting system with networking capabilities employs appropriate, well-vetted modern defenses against network-based attacks, commensurate with current best practice. (15.4)
- (U) As of March 2018, 35 states required that their machines be certified by EAC, but compliance with the VVSG standards is not mandatory. Secretary Nielsen testified before the Committee that the United States should "seek for all states" to use the VVSG standards.³¹⁴

314 (U) SSCI Transcript of the Open Hearing on Election Security, held on March 21, 2018, p. 47.

⁽U) EAC Commissioners Unanimously Vote to Publish VVSG 2,0 Principles and Guidelines for Public Comment; https://www.eac.gov/news/2019/02/15/eac-commissioners-unanimously-vote-to-publish-vvsg-20-principles-and-guidelines-for-public-comment/; February 15, 2019

VIII. (U) THE ROLE OF DHS AND INTERACTIONS WITH THE STATES

(U) The federal government's actions to address election security threats evolved significantly from the summer of 2016 through the summer of 2018. Contemporaneous with the Russian attacks, DHS and FBI were initially treating the situation as they would a typical notification of a cyber incident to a non-governmental victim. By the fall of 2016, however, DHS was attempting to do more extensive outreach to the states. Then in the fall of 2017, DHS undertook an effort to provide a menu of cyber support options to the states.

A. (U) DHS's Evolution

For DHS and other agencies and departments tasked with intelligence collection or formulating policy options through the interagency process, the full scope of the threat began to emerge in the summer of 2016. Secretary Johnson told the Committee that "I know I had significant concerns by [summer of 2016] about doing all we could to ensure the cybersecurity of our election systems." Mr. Daniel said in his interview that by the end of July, the interagency was focused on better protecting electoral infrastructure as part of a "DHS and FBI-led domestic effort." 316

Policymakers quickly realized, however, that DHS was poorly positioned to provide the kind of support states needed. Mr. Daniel said that interagency discussions about the threat "start[ed] a process of us actually realizing that, frankly, we don't actually have very much in the way of capability that we can directly offer the states"—a fact that the states themselves would later echo. 317

- Ms. Monaco said that DHS initially found a "pretty alarming variance in the number of voting registration databases and lack of encryption and lack of backup for all of these things." Ms. Monaco added that "[i]n light of what we were seeing, in light of the intelligence we were getting briefed on, this was a very specific direction and decision to say we need to really accelerate this, put a significant push on resources and engagement at the senior-most levels." 319
- Mr. Daniel and the working group identified DHS's cyber teams as possible assistance to the states. "DHS had teams that could go and provide that support to the private sector. We've been doing that. That's a program that existed for years for critical

⁽U) SSCI Transcript of the Interview with Jeh Johnson, Former Secretary of Homeland Security, held on Monday, June 12, 2017, p. 10.

³¹⁶ (U) SSCI Transcript of the Interview with Michael Daniel, Former Special Assistant to the President and Cybersecurity Coordinator, National Security Council, held on Wednesday, August 31, 2017, p. 28.
³¹⁷ (U) Ibid., p. 38.

³¹⁸ (U) SSCI Transcript of the Interview with Lisa Monaco, Former Homeland Security Advisor, held on Thursday, August 10, 2017, SSCI interview of Lisa Monaco, August 10, 2017, p. 19.
³¹⁹ (U) Ibid., p. 21.

infrastructure companies. And we realized that we could repurpose [some of those teams], but we don't have that many of them . . . four or five. It was not very many." 320

(U) DHS attempted a nuanced outreach to the states on the threat. Ms. Monaco highlighted a delicate balancing act with the interactions with states:

I know we tried very hard to strike a balance between engaging state and local officials and federal officials in the importance of raising cyber defenses and raising cybersecurity . . . and not sowing distrust in the system, both because, one, we believed it to be true that the system is in fact quite resilient because of what I mentioned earlier, which is the diffuse nature; and because we did not want to, as we described it, do the Russians' work for them by sowing panic about the vulnerability of the election. 321

- (U) In an August 15, 2016, conference call with state election officials, then-Secretary Johnson told states, "we're in a sort of a heightened state of alertness; it behooves everyone to do everything you can for your own cybersecurity leading up to the election." He also said that there was "no specific or credible threat known around the election system itself. I do not recall—I don't think, but I do not recall, that we knew about [State 4] and Illinois at that point." The Committee notes that this call was two months after State 4's system was breached, and more than a month after Illinois was breached and the state shut down its systems to contain the problem. During this call, Secretary Johnson also broached the idea of designating election systems as critical infrastructure.
- (U) A number of state officials reacted negatively to the call. Secretary Johnson said he was "surprised/disappointed that there was a certain level of pushback from at least those who spoke up. . . . The pushback was: This is our—1'm paraphrasing here: This is our responsibility and there should not be a federal takeover of the election system." 323
 - (U) The call "does not go incredibly well," said Mr. Daniel. "I was not on the call, no, but all of the reporting back and then all of the subsequent media reporting that is leaked about the call shows that it did not go well." Mr. Daniel continued: "I was actually quite surprised... in my head, there is this: yes, we have this extremely partisan election going on in the background; but the Russians are trying to mess with our election. To me, that's a national security issue that's not dependent on party or anything else." 324

324 (U) Ibid., p. 48.

^{3,0} (U) SSCI Transcript of the Interview with Michael Daniel, Former Special Assistant to the President and Cybersecurity Coordinator, National Security Council, held on Wednesday, August 31, 2017, p. 41.

⁽¹⁾ SSCI Transcript of the Interview with Lisa Monaco, Former Homeland Security Advisor, held on Thursday, August 10, 2017, p. 29.

⁽U) SSCI Transcript of the Interview with Jeh Johnson, Former Secretary of Homeland Security, held on Monday, June 12, 2017, p. 13.

^{123 (}U) Ibid., pp. 13-14.

- (U) Ms. Monaco also related how DHS received significant push back from the states and decided to "focus our efforts on really pushing states to voluntarily accept the assistance that DHS was trying to provide."³²⁵
- (U) States also reported that the call did not go well. Several states told the Committee that the idea of a critical infrastructure designation surprised them and came without context of a particular threat. Some state officials also did not understand what a critical infrastructure designation meant, in practical terms, and whether it would give the federal government the power to run elections. DHS also did not anticipate a certain level of suspicion from the states toward the federal government. As a State 17 official told the Committee, "when someone says 'we're from the government and we're here to help,' it's generally not a good thing." 326

(U) Critical Infrastructure Designation

- (U) One of the most controversial elements of the relationship between DHS and the states was the decision to designate election systems as critical infrastructure. Most state officials relayed that they were surprised by the designation and did not understand what it meant; many also felt DHS was not open to input from the states on whether such a designation was beneficial.
- (U) Secretary Johnson remembers the first time he aired the possibility of a designation was on August 3, 2016. He went to a reporters' breakfast sponsored by the Christian Science Monitor and publicly "floated the idea of designating election infrastructure as critical infrastructure." Then, on August 15, 2016, Secretary Johnson had a conference call with election officials from all 50 states. "I explained the nature of what it means to be designated critical infrastructure. It's not a mandatory set of [regulations], it's not a federal takeover, it's not binding operational directives. And here are the advantages: priority in terms of our services and the benefit of the protection of the international cyber norm." Secretary Johnson continued: "I stressed at the time that this is all voluntary and it prioritizes assistance if they seek it."
- (U) Some states were vocal in objecting to the idea. In evaluating the states' response, DHS came to the conclusion that it should put the designation on hold, deciding it would earn more state trust and cooperation if it held off on the designation as critical infrastructure and perhaps sought more buy-in from the states at a later date.³³⁰

330 (U) Ibid., p. 115.

48

³²⁸ (U) SSCI Transcript of the Interview with Lisa Monaco, Former Homeland Security Advisor, held on Thursday, August 10, 2017, SSCI interview of Lisa Monaco, August 10, 2017, p. 25.

¹²⁶ (U) Memorandum for the Record, SSCI Staff, Conference Call with State 17, January 25, 2018.

³²⁷ (U) SSCI Transcript of the Interview with Jeh Johnson, Former Secretary of Homeland Security, held on Monday, June 12, 2017, p. 10.

³²⁸ (U) *Ibid.*, p. 14. For additional information on the definition of critical infrastructure in a cybersecurity context, see Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, February 12, 2013.

^{329 (}U) SSCI Transcript of the Open Hearing on Election Security, March 21, 2018, p. 34.

- (U) After the election, Secretary Johnson decided the time had come to make the designation. He held a follow-up call with NASS on the critical infrastructure designation in January 2017: "I didn't tell them I'm doing this the next day, but I told them I was close to making a decision. I didn't hear anything further [along the lines of additional, articulated objections], so the same day we went public with the [unclassified] version of the report, 334 I also made the designation." 332
- (U) Mr. Daniel summed up the rationale for proceeding this way: "I do believe that we should think of the electoral infrastructure as critical infrastructure, and to me it's just as critical for democracy as communications, electricity, water. If that doesn't function, then your democracy doesn't function. . . . To me that is the definition of 'critical.'"333
- (U) In interviews with the Committee in late 2017 and early 2018, several states were supportive of the designation and saw the benefits of, for example, the creation of the Government Coordinating Council. Others were lukewarm, saying they had seen limited benefits for all the consternation officials said it had caused. Still others remained suspicious that the designation is a first step toward a federal takeover of elections.

B. (U) The View From the States

(U) For most states, the story of Russian attempts to back state infrastructure was one of confusion and a lack of information. It began with what states interpreted as an insignificant event: an FBI FLASH notification on August 18, 2016,

334 Then, in mid-October, the MS-ISAC reached out to state IT directors with an additional alert about specific IP addresses scanning websites.

At no time did MS-ISAC or DHS identify the IP addresses as associated with a nation-state actor. Given the lack of context, state staff who received the notification did not ascribe any additional urgency to the warning; to them, it was a few more suspect IP addresses among the thousands that were constantly pinging state systems. Very few state IT directors informed state election officials about the alert.

334 (U) FBI FLASH, Alert Number T-LD1004-TT, TLP-AMBER,

) FBI FLASH, Alert Number T-LD1005-TT, TLP-AMBER,

DHS/FBL JAR-16-20223. Threats to Federal

State, and Local Government Systems, October 14, 2016.

40

^{331 (}U) Secretary Johnson was referring to the declassified version of the Intelligence Community Assessment, Assessing Russian Activities and Intentions in Recent U.S. Elections, January 6, 2017.

³³² (U) *Ibid.*, p. 46.

³⁴³ (U) SSCI Transcript of the Interview with Michael Daniel, Former Special Assistant to the President and Cybersecurity Coordinator, National Security Council, held on Wednesday, August 31, 2017, p. 98.

- (U) State 11 had a meeting with DHS officials, including the regional DHS cyber advisor, in August 2016, but according to State 11 officials, DHS did not mention any specific threat against election systems from a nation-state actor.³³⁶
- (U) State 13 reported that DHS contacted an affected county at one point, but never contacted the state-level officials.³³⁷
- (U) When they saw an IP address identified in the alerts had scanned their systems, State 6 and State 16 sent their logs to the MS-ISAC for analysis.³³⁸ State 16 said it never received a response.³³⁹
- (U) DHS, conversely, saw its efforts as far more extensive and effective. Ms. Manfra testified to SSCI that DHS "held a conference call where all 50 secretaries of state or an election director if the secretary of state didn't have that responsibility [participated], in August, in September, and again in October [of 2016], both high-level engagement and network defense products [sic]." Mr. Daniel reported that "by the time Election Day rolls around, all but one state has taken us up on the offer to at least do scanning [,] so I want to give people credit for not necessarily sticking to initial partisan reactions and . . . taking steps to protect their electoral infrastructure." ³⁴¹
- (U) States reported to the Committee that Election Day went off smoothly. For most state election officials, concerns about a possible threat against election systems dropped off the radar until the summer or fall of 2017. Many state election officials reported hearing for the first time that Russian actors were responsible for scanning election infrastructure in an estimated 21 states from the press or from the Committee's open hearing on June 21, 2017. During that hearing, in response to a question from Vice Chairman Warner inquiring whether all affected states were aware they were attacked, Ms. Manfra responded that "[a]ll of the system owners within those states are aware of the targeting, yes, sir." However, when pressed as to whether election officials in each state were aware, the answer was less clear.
 - (U) In that hearing, Dr. Liles said DHS had "worked hand-in-hand with the state and local partners to share threat information related to their networks." 344

50

^{336 (}U) Memorandum for the Record, SSCI Staff, Conference Call with [State 11], December 8, 2017.

^{337 (}U) Memorandum for the Record, SSCI Staff, Conference Call with [State 13], December 1, 2017.

^{338 (}U) Memorandum for the Record, SSCI Staff, Conference Call-with [State 6], November 17, 2017; Memorandum for the Record, SSCI Staff, Conference Call with [State 16], December 1, 2017.

^{339 (}U) Ibid. State 6 did not indicate whether they received feedback from DHS.

⁵⁴⁰ (U) SSCI Transcript of the Open Hearing on Russian Interference in the 2016 U.S. Elections, June 21, 2017, p. 74.

³⁴¹ (U) SSCI Transcript of the Interview with Michael Daniel, Former Special Assistant to the President and Cybersecurity Coordinator, National Security Council, held on Wednesday, August 31, 2017, p. 49.

^{342 (}U) SSC1 Transcript of the Open Hearing on Russian Interference in the 2016 U.S. Elections, held on Wednesday, June 21, 2017, p. 28.

^{343 (}U) Ibid., pp. 62-63.

^{344 (}U) Ibid., p. 12.

- (U) Ms. Manfra said, "The owners of the systems within those 21 states have been notified." Senator King then asked, "How about the election officials in those states?" Ms. Manfra responded, "We are working to ensure that election officials as well understand. I'll have to get back to you on whether all 21 states[crosstalk]."³⁴⁵
- (U) Given Ms. Manfra's testimony and the fact that some election officials did not get a
 notification directly to their offices, election officials in many states assumed they were
 not one of the 21; some even issued press releases to that effect.³⁴⁶
- (U) The disconnect between DHS and state election officials became clear during Committee interactions with the states throughout 2017. In many cases, DHS had notified state officials responsible for network security, but not election officials, of the threat. Further, the IT professionals contacted did not have the context to know that this threat was any different than any other scanning or hacking attempt, and they had not thought it necessary to elevate the warning to election officials.
- (U) After the hearing, and in part to respond to confusion in the states, DHS held a conference call with representatives from 50 states in September 2017. In that call, DHS said they would contact affected states directly. State 8 state election officials noted that the call became "somewhat antagonistic." State 17 officials reported that the phone call "just showed how little DHS knew about elections." Several officials argued that all 50 states should be notified of who had been hacked. DHS followed up with one-to-one phone calls to states over the next several days.
 - (U) Officials from some states reported being shocked that they were in fact one of the states, and further surprised that their states had supposedly been notified.
 - (U) Most state officials found the conference calls lacking in information and were left wondering exactly what the threat might be. Several states said the DHS representatives could not answer any specific questions effectively.
- (U) Following this series of difficult engagements, DHS set about trying to build relationships with the states, but it faced a significant trust deficit. Early follow-up interactions between state election officials and DHS were rocky. States reported that DHS seemed to have little to no familiarity with elections. For example, State 6 said that the DHS representatives they were assigned seemed to know nothing about State 6, and, when pressed, they admitted they were "just reading the spreadsheet in front of [them]." State 8 reported that "we are spending

^{345 (}U) Ibid., pp. 62-63.

³⁴⁶ (U) State 8 said they put out a press release because DHS had said publicly that they had notified the 21 states, and "if you were one of the 21, you would know."

^{347 (}U) Memorandum for the Record, SSCI Staff, Conference Call with [State 8], February 2, 2018.

³⁴⁸ (U) Memorandum for the Record, SSCI Staff, Conference Call with [State 17], January 25, 2018.

³⁴⁹ (U) Memorandum for the Record, SSCI Staff, Conference Call with [State 6], November 17, 2017.

a ton of time educating outside groups on how elections are run."³⁵⁰ State 3 officials said, "DHS didn't recognize that securing an election process is not the same as securing a power grid."³⁵¹

- (U) By early 2018, State officials gave DHS credit for making significant progress over the next six months. States began to sign up for many of the resources that DHS had to offer, and DHS hosted the first meeting of the Government Coordinating Council required under the critical infrastructure designation. Those interactions often increased trust and communication between the federal and state entities. For example, DHS has identified a list of contacts to notify if they see a threat; that list includes both IT officials and election officials. State 9 described it as "quite a turnaround for DHS," and further stated that the Secretaries of State had been disappointed with how slowly DHS got up to speed on election administration and how slowly the notifications happened, but DHS was "quick with the *mea culpas* and are getting much better." 352
- (U) Not all of the engagements were positive, however. State 13 in early December 2017 still reported continued frustration with DHS, indicating to the Committee that it had not seen much change in terms of outreach and constructive engagement. As of summer 2017, according to State 13, "the lack of urgency [at DHS] was beyond frustrating." 353

C. (U) Taking Advantage of DHS Resources

(U) As DHS has pursued outreach to the states, more and more have opened their doors to DHS assistance. DHS told the Committee that its goal has been relationship building and:

In the partnerships with the states and secretaries of states, state election directors, and at the local level, we're trying to shift them to a culture of more information security management, where they can now account for the integrity of their system, or, if something did happen . . . they know the full extent of what happened on their system. . . . We're providing vulnerability assessments and trend analysis, in addition to connecting them to the threat intelligence that we can, in order to evolve their . . . cyber culture. 354

(U) DHS's assistance can be highly tailored to need, and falls into roughly two buckets: remote cyber hygiene scans, which provide up to weekly reports, and on-site risk and vulnerability assessments. DHS also offers a suite of other services, including phishing campaign assessments. All these efforts seek to provide the states with actionable information to improve cyber hygiene, but DHS has been keen to avoid what could be perceived by the states as

^{350 (}U) Memorandum for the Record, SSCl Staff, Conference Call with [State 8], February 2, 2018.

^{351 (}U) Memorandum for the Record, SSCI Staff, Conference Call with [State 3], December 8, 2017.

^{352 (}U) Memorandum for the Record, SSCI Staff, Conference Call with [State 9], November 17, 2017.

^{353 (}U) Memorandum for the Record, SSCI Staff, Conference Call with [State 13], December 1, 2017.

^{354 (}U) SSCI interview with DHS and CTIIC, February 27, 2018, pp. 54-55.

unfunded mandates.³⁵⁵ Some states requesting more intensive services have also experienced significant delays before DHS could send a team to assist.

- (U) By October 2018, DHS said 35 states, 91 local jurisdictions, and eight election system vendors had signed up for remote persistent scans.³⁵⁶ All the requests for these scans have been fulfilled. "They can be turned on basically within the week," according to DHS.³⁵⁷
- (U) DHS said that as of October 2018, it had completed 35 in-depth, on the ground vulnerability assessments: 21 states, 13 localities, and one election system vendor. These assessments are one week off-site remote scans followed by a second week on site. 358
- (U) Two states who completed the in-depth assessments reported in late 2017 they had had a good experience. State 12 officials said the team was "extremely helpful and professional." State 10 said the review was a good experience, although DHS was somewhat limited in what it could do. For example, DHS did a phishing email test that showed the training for employees had worked. DHS gave "good and actionable recommendations." Although DHS "didn't really understand election systems when they came," they learned a lot. 362
- (U) As of November 2017, State 6 and State 9 requested an on-site scan, but those scans were on track to be delayed past the August 2018 primaries.³⁶³ State 7 was expecting a four-to-six month delay.³⁶⁴ State 8 signed up for a checkup in October 2017 and was due to get service the following February.³⁶⁵ As of January 2018, State 17 also had requested an on-site scan.³⁶⁶
- (U) In a sign of improving relations between the states and DHS, two states that had elections in 2017 attempted to include DHS in the process more extensively than in the past. In State 17, a two-person DHS team sat with election officials during the 2017 special election and monitored the networks. Even though "their presence was comforting," they "really didn't do much." State 17 signed DHS's normal MOU, but also added its own clause to underscore the state's independence: a formal sunset on DHS's access to state systems, one week after the

^{355 (}U) Ibid., p. 60.

^{356 (}U) Ibid., p. 57.

^{367 (}U) DHS phone call with SSCI; October 16, 2018.

^{358 (}U) Ibid

^{359 (}U) Memorandum for the Record, SSCI Staff, Conference Call with [State 12], December 1, 2017.

^{360 (}U) Ibid.

^{361 (}U) Ibid.

^{362 (}U) Ibid.

³⁶³ (U) Memorandum for the Record, SSCI Staff, Conference Call with [State 6], November 17, 2017; Memorandum for the Record, SSCI Staff, Conference Call with [State 9], November 17, 2017.

^{364 (}U) Memorandum for the Record, SSCI Staff, Conference Call with [State 7], January 25, 2018.

^{365 (}U) Memorandum for the Record, SSCI Staff, Conference Call with [State 8], February 2, 2018.

³⁶⁶ (U) Memorandum for the Record, SSCI Staff, Conference Call with [State 17], January 25, 2018.

election. State 7 reported their experience with DHS during the 2017 statewide election was quite good. DHS sat with election officials all day, which meant State 7 could pass messages quickly to NCCIC.

(U) In March 2018, Congress appropriated \$380 million in funding for election security improvements. The funding was distributed under the formula laid out in the Help American Vote Act (HAVA) and was intended to aid in replacing vulnerable voting machines and improving cybersecurity. As of July 2018, 13 states said they intended to use the funds to buy new voting machines, and 22 said they have "no plans to replace their machines before the election—including all five states that rely solely on paperless electronic voting devices," according to a survey by Politico.³⁶⁷

IX. (U) RECOMMENDATIONS

- 1. (U) Reinforce States' Primacy in Running Elections*
- (U) States should remain firmly in the lead on running elections, and the federal government should ensure they receive the necessary resources and information.
 - 2. (U) Build a Stronger Defense, Part 1: Create Effective Deterrence
- (U) The United States should communicate to adversaries that it will view an attack on its election infrastructure as a hostile act, and we will respond accordingly. The U.S. Government should not limit its response to cyber activity; rather, it should create a menu of potential responses that will send a clear message and create significant costs for the perpetrator.

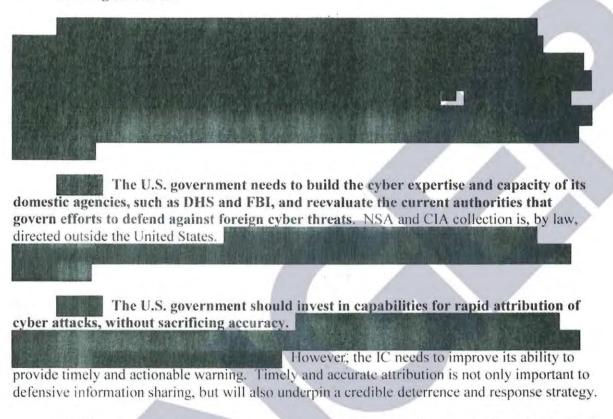
Ideally, this principle of deterrence should be included in an overarching cyber doctrine for the U.S. Government. That doctrine should clearly delineate cyberespionage, cybercrime, and cyber attacks. Further, a classified portion of the doctrine should establish what the U.S. Government believes to be its escalation ladder in the cyber realm—what tools does it have, what tools should it pursue, and what should the limits of cyber war be. The U.S. strategic approach tends to overmatch adversaries with superior technology, and policymakers should consider what steps the U.S. will need to take to outstrip the capabilities of Russia, China, Iran, North Korea, and other emerging hostile actors in the cyber domain.

(U) U.S. cyber doctrine should serve as the basis for a discussion with U.S. allies and others about new cyber norms. Just as the international community has established norms and treaties about the use of technologies and weapons systems, the U.S. should lead a conversation about cyber norms and the limits of cyber activity with allies and others.

[&]quot;The Committee's recommendation to "reinforce states' primacy in running elections" should be understood in reference to states' responsibility for election security, and not as pertaining to broader election issues, such as campaign finance laws or voting rights laws.

³⁶⁷ (U) States Slow to Prepare for Hacking Threats, Eric Geller, Politico, July 18, 2018.

3. (U) Build a Stronger Defense, Part II: Improve Information Gathering and Sharing on Threats



- (U) The federal government and state governments need to create clear channels of communication two ways—down from the federal government to the state and local level, and up from the state and local officials on the front lines to federal entities. In 2016, DHS and FBI did not provide enough information or context to election officials about the threat they were facing, but states and DHS have made significant progress in this area in the last two years. For example, Secretary of Homeland Security Nielsen testified to the Committee in March 2018 that "today I can say with confidence that we know whom to contact in every state to share threat information. That capability did not exist in 2016." 369
- (U) A key component of information sharing about elections is security clearances for appropriate officials at the state and local level. DHS and its partners can effectively strip classified information off of cyber indicators, which can then be passed to technical staff at the state level, but in order for those indicators to not get lost in the multitude of cyber threats those professionals see on a daily basis, senior officials at the state and local levels need to know the

(U) SSCI Transcript of the Open Hearing on Election Security, held on March 21, 2018, p. 16.

context surrounding the indicators. State officials need to know why a particular threat is of significant concern, and should be prioritized. That context could come from classified information, or states could come to understand that threat information DHS passes them is more serious than that received through other sources. DHS's goal is to obtain clearances for up to three officials per state.³⁷⁰ As of August 2018, DHS had provided a clearance to 92 officials³⁷¹; as of late 2017 all state election officials had received interim secret clearances or one-day readins for secret-level briefings.³⁷² DHS, along with ODNI and FBI, also hosted state and local election officials for a SECRET-level briefing on the sidelines of the biannual NASS and NASS-ED conferences in Washington, DC in February 2018. In March, Amy Cohen, Executive Director of NASS-ED testified in front of the Committee that, "It would be naïve to say that we received answers to all our questions, but the briefing was incredibly valuable and demonstrated how seriously DHS and others take their commitment to the elections community as well as to our concerns." The Committee recommends DHS continue providing such briefings and improve the quality of information shared.

- (U) Fundamental to meaningful information sharing, however, is that state officials understand what they are getting. New inductees to the world of classified information are often disappointed—they expected to see everything laid out in black and white, when intelligence is often very gray, with a pattern discernable only to those who know where to look and what conclusions to draw. Those sharing the intelligence should manage expectations—at the SECRET level, officials are likely to see limited context about conclusions, but not much more.
- (U) Federal officials should work to declassify information, for the purpose of providing warning to appropriate state and local officials, to the greatest extent possible. If key pieces of context could be provided at a lower classification level while still protecting classified information, DHS and its partners should strive to do so.
 - 4. (U) Build a Stronger Defense, Part III: Secure Election-Related Cyber Systems
- (U) Despite the expense, cybersecurity needs to become a higher priority for election-related infrastructure. The Committee found a wide range of cybersecurity practices across the states. Some states were highly focused on building a culture of cybersecurity; others were severely under-resourced and relying on part-time help.
- (U) The Committee recommends State officials work with DHS to evaluate the security of their election systems end-to-end and prioritize implementing the following steps to secure voter registration systems, state records, and other pre-election activities. The Committee additionally recommends that State officials:

³⁷⁰ (U) SSCI Transcript of the Open Hearing on Election Security, held on March 21, 2018, p.15.

⁽U) DTS 2018-3275, Summary of 8/22/2018 All Senators Election Security Briefing, August 28, 2018.

⁽U) SSC1 Transcript of the Open Hearing on Election Security, held on March 21, 2018, p 15, 26.

³⁷³ (U) SSCI Transcript of the Open Hearing on Election Security, held on March 21, 2018, p.113.

- (U) Identify the weak points in their networks, like under-resourced localities. State 7 said they are not worried about locations like larger counties when it comes to network security, but they are worried about "the part-time registrar who is also the town attorney and the town accountant and is working out of a 17th century jail." 374
- (U) Undertake security audits of state and local voter registration systems, ideally
 utilizing private sector entities capable of providing such assistance. State and local
 officials should pay particular attention to the presence of high severity vulnerabilities in
 relevant web applications, as well as highly exploitable vulnerabilities such as cross-site
 scripting and SQL injection.
- (U) Institute two-factor authentication for user access to state databases.
- (U) Install monitoring sensors on state systems. As of mid-2018, DHS's ALBERT sensors covered up to 98% of voting infrastructure nationwide, according to Undersecretary Krebs.³⁷⁵
- (U) Include voter registration database recovery in state continuity of operations plans.
- (U) Update software in voter registration systems. One state mentioned that its voter registration system is more than ten years old, and its employees will "start to look for shortcuts" as it gets older and slower, further imperiling cybersecurity.
- (U) Create backups, including paper copies, of state voter registration databases.
- (U) Consider a voter education program to ensure voters check registration information well prior to an election.
- (U) DHS in the past year has stepped up its ability to assist the states with some of these activities, but DHS needs to continue its focus on election infrastructure and pushing resources to the states.
 - (U) The Committee recommends DHS take the following steps:
 - (U) Create an advisory panel to give DHS expert-level advice on how states and localities run elections. The Government Coordinating Council, created as part of the critical infrastructure designation, could serve as a venue for educating DHS on what states do and what they need.

^{374 (}U) Memorandum for the Record, SSCI Staff, Conference Call with [State 7], January 25, 2018.

^{373 (}U) DTS 2018-3275, Summary of 8/22/2018 All Senators Election Security Briefing, August 28, 2018.

- (U) Create guidelines on cybersecurity best practices for elections and a public awareness campaign to promote election security awareness, working through EAC, NASS, and NASED, and with the advisory panel.
- (U) Develop procedures and processes to evaluate and routinely provide guidance on relevant vulnerabilities associated with voting systems in conjunction with election experts.
- (U) DHS has already created a catalog of services they can provide to states to help secure states' systems. DHS should maintain the catalog and continue to update it as it refines its understanding of what states need.
- (U) Expand capacity so wait times for services, like voluntary vulnerability assessments, are manageable and so that DHS can maintain coverage on other critical infrastructure sectors. Robbing resources from other critical infrastructure sectors will eventually create unacceptable new vulnerabilities.
- (U) Work with GSA to establish a list of approved private-sector vendors who can
 provide services similar to those DHS provides. States report being concerned about
 "vultures" —companies who show up selling dubious cyber solutions. That being said,
 some states will be more comfortable having a private sector entity evaluate their state
 systems than a federal agency.
- (U) Continue to build the resources of the newly established EI-ISAC. States have already found this information sharing service useful, and it could serve as a clearinghouse for urgent threat information. As of August 2018, the EI-ISAC had over 1,000 members with participants in all 50 states.³⁷⁶
- (U) Continue training for state and local officials, like the table-top exercise conducted
 in August of 2018 that brought together representatives from 44 states, localities, and the
 federal government to work through an election security crisis.³⁷⁷ The complexity of the
 scenario encouraged state and local officials to identify serious gaps in their preparations
 for Election Day.
- 5. (U) Build a Stronger Defense, Part IV: Take Steps to Secure the Vote Itself
- (U) Given Russian intentions to undermine the credibility of the election process, states should take urgent steps to replace outdated and vulnerable voting systems. When safeguarding the integrity of U.S. elections, all relevant elements of the government—including at the federal, state, and local level—need to be forward looking and work to address vulnerabilities before they are exploited.

377 (U) DHS, Press release: DHS Hosts National Exercise on Election Security, August 15, 2018.

^{376 (}U) DTS 2018-3275, Summary of 8/22/2018 All Senators Election Security Briefing, August 28, 2018.

- (U) As states look to replace HAVA-era machines that are now out of date, they should
 purchase more secure voting machines. Paper ballots and optical scanners are the least
 vulnerable to cyber attack; at minimum, any machine purchased going forward should
 have a voter-verified paper trail and remove (or render inert) any wireless networking
 capability.
- (U) States should require that machines purchased from this point forward are either EAC certified or comply with the VVSG standards. State purchasers should write contracts with vendors to ensure adherence to the highest security standards and to demand guarantees the supply chains for machines are secure.
- (U) In concert with the need for paper ballots comes the need to secure the chain of
 custody for those ballots. States should reexamine their safeguards against insertion of
 fraudulent paper ballots at the local level, for example time stamping when ballots are
 scanned.
- (U) Statistically sound audits may be the simplest and most direct way to ensure confidence in the integrity of the vote. The states should begin to implement audits of election results. Logic and accuracy tests of machines are a common step, but do not speak to the integrity of the actual vote counting. Risk-limiting audits, or some similarly rigorous alternative, are the future of ensuring that votes cast are votes counted. State 8, State 12, State 21, State 9, State 2, State 16, and others already audit their results, and others are exploring additional pilot programs. However, as of August 2018, five states conducted no post-election audit and 14 states do not do a complete post-election audit. The Committee recognizes states' concern about the potential cost of such audits and the necessary changes to state laws and procedures; however, the Committee believes the benefit of having a provably accurate vote is worth the cost.
- (U) States should resist pushes for online voting. One main argument for voting online
 is to allow members of the military easier access to their fundamental right to vote while
 deployed. While the Committee agrees states should take great pains to ensure members

³⁷⁸ (U) Election experts point out, however, that audits could create a new vector for election-related lawsuits. Complainants could allege that the audit was done improperly, or that the audit process reflected bias.

^{379 (}U) State 8 passed a law to audit starting in 2018, with random precinct sampling. State 12 does state-wide audits. State 21 audits 2% of ballots, randomly selected. State 9 picks 210 of 4100 precincts at random for an audit. State 2 hand-counts ballots in randomly selected precincts and uses automated software to test. A States law on ballot storage can't accommodate risk-limiting audits. Instead, they use ClearBallot software. They upload images of ballots to an external hard drive and send it to ClearBallot. ClearBallot is blind to who won and independently evaluates the results. In addition, the company can identify problems with scanners; for example, when a fold in absentee ballots recorded as a vote. Cybersecurity experts still doubt, however, that this type of procedure is secure.

^{380 (}U) DTS 2018-3275, Summary of 8/22/2018 All Senators Election Security Briefing, August 28, 2018.

of the military get to vote for their elected officials, no system of online voting has yet established itself as secure. 381

- (U) DHS should work with vendors of election equipment to educate them about the
 vulnerabilities in both the machines and the supply chains for the components of their
 machines. Idaho National Lab is already doing some independent work on the security of
 a select set of voting machines, developing a repeatable methodology for independently
 testing the security of such systems.
- (U) The Department of State should work with FBI and DHS to warn states about foreign efforts to access polling places outside normal channels in the future and remain vigilant about rejecting aberrant attempts.
- (U) The Associated Press is responsible for reporting unofficial, initial election results on
 election night and is a critical part of public confidence in the voting tally. States and
 DHS should work with the AP and other reporting entities to ensure they are both secure
 and reporting accurate results.
- (U) The Committee found that, often, election experts, national security experts, and
 cybersecurity experts are speaking different languages. Election officials focus on
 transparent processes and open access and are concerned about introducing uncertainty
 into the system; national security professionals tend to see the threat first. Both sides
 need to listen to each other better and to use more precise language.

6. (U) Assistance for the States

- (U) State officials told the Committee the main obstacle to improving cybersecurity and purchasing more secure voting machines is cost. State budgets are stretched thin by priorities that seem more urgent on a daily basis and are far more visible to constituents.
- (U) In March 2018, Congress appropriated \$380 million in funds under the HAVA formula for the states. As of August 2018, states had begun to allocate and spend that money for items such as cybersecurity improvements.
- (U) The Committee recommends the EAC, which administers the grants, regularly report to Congress on how the states are using those funds, whether more funds are needed, and whether states have both replaced outdated voting equipment and improved

⁽U) Dr. Halderman in his testimony before the Committee said, "I think that online voting, unfortunately, would be painting a bullseye on our election system. Today's technology just does not provide the level of security assurance for an online election that you would need in order for voters to have high confidence. And I say that having myself'... hacked an online voting system that was about to be used in real elections, having found vulnerabilities in online voting systems that are used in other countries. The technology just isn't ready for use." See SSC1 Transcript of the Open Hearing on Russian Interference in the 2016 U.S. Elections, held on Wednesday, June 21, 2017, p. 152.

cybersecurity. More funds may be needed, as the allocation under the HAVA formula did not prioritize replacing vulnerable electronic-only machines.

- (U) States should be able to use grant funds to improve cybersecurity in a variety of
 ways, including hiring additional IT staff, updating software, and contracting with
 vendors to provide cybersecurity services. "Security training funded and provided by a
 federal entity such as the EAC or DHS would also be beneficial in our view," 382 an
 official from Illinois testified.
- (U) Funds should also be available to defray the cost of instituting audits.
- (U) States with vulnerable DRE machines with no paper backup should receive urgent access to funding. Dr. Halderman testified that replacing insecure paperless voting machines nationwide would cost \$130 to \$400 million dollars. Risk-limiting audits would cost less than \$20 million a year. 383



³⁸² (U) SSCI Transcript of the Open Hearing on Russian Interference in the 2016 U.S. Elections, held on Wednesday, June 21, 2017, p. 114.
³⁸³ (U) *Ibid.*, p. 119.

61 COMMITTEE SENSITIVE - RUSSIA INVESTIGATION ONLY

MINORITY VIEWS OF SENATOR WYDEN

(U) The role of the federal government

- (U) The Committee report describes Russian attacks on U.S. election infrastructure in 2016 and lays out many of the serious vulnerabilities that exist to this day. These vulnerabilities pose a direct and urgent threat to American democracy which demands immediate congressional action. The defense of U.S. national security against a highly sophisticated foreign government cannot be left to state and county officials. For that reason, I cannot support a report whose top recommendation is to "reinforce[] state's primacy in running elections."
- (U) Congress's constitutional role in regulating federal elections is well-established. In response to an inquiry from the bipartisan leadership of the U.S. Senate, the General Accounting Office (GAO) wrote that "[w]ith regard to the administration of federal elections, Congress has constitutional authority over both congressional and presidential elections." Indeed, pursuant to the Elections Clause of the U.S. Constitution, Congress's authority over congressional elections is "paramount to that of the states." As the GAO report details, Congress has repeatedly passed legislation related to the administration of elections on topics such as the timing of federal elections, voter registration, absentee voting requirements, disability access, and voting rights.
- (U) If there was ever a moment when Congress needed to exercise its clear constitutional authorities to regulate elections, this is it. America is facing a direct assault on the heart of our democracy by a determined adversary. We would not ask a local sheriff to go to war against the missiles, planes and tanks of the Russian Army. We shouldn't ask a county election IT employee to fight a war against the full capabilities and vast resources of Russia's cyber army. That approach failed in 2016 and it will fail again. The federal government's response to this ongoing crisis cannot be limited offers to provide resources and information, the acceptance of which is voluntary. If the country's elections are to be defended, Congress must also establish mandatory, nation-wide cybersecurity requirements.

(U) Security of voting machines

(U) Experts are clear about the measures necessary to protect U.S. elections from cyber manipulation.³ Absent an accessibility need, most voters should hand-mark paper ballots. For voters with some kind of need, ballot marking devices that print paper ballots should be available. Risk-limiting audits must be also be required. Currently, however, only Virginia, Colorado and Rhode Island meet these requirements.⁴ These critical reforms must be adopted

¹ "Elections. The Scope of Congressional Authority in Election Administration," General Accounting Office, March 2001, prepared in response to a joint inquiry from Senator Trent Lott, Republican Leader; Senator Tom Daschle, Democratic Leader; Senator Mitch McConnell, Chairman, and Senator Christopher Dodd, Ranking Member, of the Senate Committee on Rules and Administration.

² Article I, Section 4, Clause 1

³ Securing the Vote; Protecting American Democracy; National Academy of Sciences, Engineering and Medicine, September 2018

⁴ National Conference of State Legislatures, Post-Election Audits, January 3, 2019. Verifiedvoter.org. The Verifier – Polling Place Equipment – November 2018. Oregon requires paper ballots and the Oregon State Senate has passed a bill requiring risk-limiting audits.

throughout the country, which is why, on June 27, 2019, the House of Representatives passed H.R. 2722, the Securing America's Federal Elections (SAFE) Act. The security of the country's voting machines depends on this legislation being signed into law.

- (U) The Committee, in recommending basic security measures like paper ballots and audits, notes that there is currently "a wide range of cybersecurity practices across the states." Indeed, the data is deeply concerning and highlights the need for mandatory, nation-wide standards. For example, the Committee rightly highlights the vulnerabilities of Direct-Recording Electronic (DRE) Voting Machines, noting that, without a paper trail, there would be no way to conduct a meaningful "recount" and compromises would remain undetected. As of November 2018, however, there were still four states in which every single county relied on DREs without voter verified paper audit trail printers (VVPAT) and, in an additional eight states, there were multiple counties that relied on DREs without a VVPAT. Gaps in the deployment of VVPATs, which are far less secure than hand-marked paper ballots, demonstrate that even bare minimum security best practices are not being met in many parts of the country.
- (U) In addition, 16 states have no post-election audits of any kind, while many others have insufficient or perfunctory audits. Only four states have a statutory requirement for risk-limiting audits, while two states provide options for counties to run different kinds of audits, one of which is a risk-limiting audit.⁶ Next year, a third state will provide that option. In other words, the vast majority of states have made no moves whatsoever toward implementing minimum standards that experts agree are necessary to guarantee the integrity of elections.
- (U) The Committee rightly identifies problems with vendors of voting machines, noting vulnerabilities in both the machines and the supply chains for machine components. Currently, however, the federal government has no regulatory authority that would require these vendors to adhere to basic security practices. Only general federal requirements that states and localities use paper ballots and conduct audits will ensure that the risk posed by voting machines provided by private vendors to states and localities can be contained. The stakes could not be more clear. As Homeland Secretary Kirstjen Nielsen testified to the Committee, "If there is no way to audit the election, that is absolutely a national security concern."

(U) Registration databases and election night reporting websites

(U) Two additional components of the U.S. election infrastructure require immediate, mandatory cybersecurity fixes. The first are voter registration databases. The Committee received testimony about successful Russian exfiltration of databases of tens of thousands of voters. Expert witnesses also described the chaos that manipulated voter registration data could cause should voters arrive at the polls and find that their names had been removed from the rolls.

⁵ Verifiedvoter.org. The Verifier – Polling Place Equipment – November 2018.

⁶ The four states are Colorado, Nevada, Rhode Island, and Virginia. National Conference of State Legislatures, Post-Election Audits, January 3, 2019.

⁷ Testimony of Homeland Security Secretary Kirstjen Nielsen, March 21, 2018.

⁸ Testimony of Homeland Security Secretary Kirstjen Nielsen, March 21, 2018.

⁹ Testimony of Connie Lawson, President-elect, National Association of Secretaries of State, and Secretary of State, State of Indiana; testimony of Steve Sandvoss, Executive Director of Illinois State Board of Elections, June 21, 2017; Illinois Voter Registration System Database Breach Report.

As one expert testified, this form of interference "could be used to sabotage the election process on Election Day." ¹⁰

- (U) The Committee report describes a range of cybersecurity measures needed to protect voter registration databases, yet there are currently no mandatory rules that require states to implement even minimum cybersecurity measures. There are not even any voluntary federal standards.
- (U) An additional component of the U.S. election infrastructure that requires immediate, mandatory cybersecurity measures are the election night reporting websites run by the states. The Committee heard testimony about a Russian attack on Ukraine's web page for announcing results. That attacked allowed the Russians to use misinformation that left Ukraine in chaos for days after the election. As the Committee's expert witness warned, "[w]e need to look at that playbook. They will do it to us." Like voter registration databases, election results websites are not subject to any mandatory standards. Both of these critical vulnerabilities, as well as vulnerabilities of voting machines, must be addressed by the U.S. Congress through the passage of S. 2238, the Senate version of the SAFE Act.
- (U) Given the inconsistent, and at times non-existent adherence to basic cybersecurity among states and localities, I cannot agree with the Committee's conclusion that "the country's decentralized election system can be a strength from a cybersecurity perspective." Until election security measures are required of every state and locality, there will be vulnerabilities to be exploited by our adversaries. The persistence of those vulnerabilities has national consequences. The manipulation of votes or voter registration databases in any county in the country can change the result of a national election. The security of the U.S. election system thus hinges on its weakest links the least capable, least resourced local election offices in the country, many of which do not have a single full-time employee focused on cybersecurity.
- (U) Every American has a direct stake in the cybersecurity of elections throughout the country. Congress has an obligation to protect the country's election system everywhere. If there were gaps in the defense of our coastline or air space, members would ensure that the federal government close them. Vulnerabilities in the country's election cybersecurity require the same level of national commitment.

(U) Cybersecurity vulnerabilities and influence campaigns

(U) The cybersecurity vulnerabilities of the U.S. election system cannot be separated from Russia's efforts to influence American voters. As the January 2017 Intelligence Community Assessment (ICA) concluded, and as the Committee report notes, the Russians were "prepared to publicly call into question the validity of the results" and "pro-Kremlin bloggers had prepared a Twitter campaign, #DemocracyRIP, on election night in anticipation of Secretary Clinton's victory." This plan highlights an additional reason why nation-wide election cybersecurity standards are so critical. If Russia's preferred candidate does not prevail in the 2020 election, the

¹⁰ Testimony of Alex J. Halderman, Professor of Computer Science and Engineering, University of Michigan, June 21, 2017.

¹¹ Testimony of Eric Rosenbach, Co-Director of the Belfer Center for Science and International Affairs, Harvard Kennedy School, March 21, 2018.

Russians may seek to delegitimize the election. The absence of any successful cyber intrusions, exfiltrations or manipulations would greatly benefit the U.S. public in resisting such a campaign.

- (U) While not formally part of the U.S. election infrastructure, the devices and accounts of candidates and political parties represent an alarming vulnerability in the country's overall election system. Russia's campaign of hacking the emails of prominent political figures and releasing them through Wikileaks, Gucifer 2.0, and DCLeaks was probably its most effective means of influencing the 2016 election. The Committee has received extensive testimony about these operations, the vulnerabilities that allowed them to occur, and the threat those vulnerabilities pose to the integrity of American democracy. Yet little has been done to prevent it from happening all over again. S. 1569, the Federal Campaign Cybersecurity Assistance Act of 2019, addresses these vulnerabilities head on by authorizing political committees to provide cybersecurity assistance to candidates, campaigns and state parties.
- (U) These vulnerabilities extend to the U.S. Senate, most of whose members are or will be candidates for reelection or for other positions. As a November 2018 Senate report noted, there is "mounting evidence that Senators are being targeted for hacking, which could include exposure of personal data." Private communications and information reside on personal accounts and devices. Passage of S. 890, the Senate Cybersecurity Protection Act, will authorize the Senate Sergeant at Arms to protect the personal devices and accounts of Senators and their staff and help prevent the weaponization of their data in campaigns to influence elections.

(U) Assessments related to the 2016 election

- (U) I have also submitted these Minority Views to address assessments related to Russian activities during the 2016 election. According to the January 2017 ICA, DHS assessed that "the types of systems we observed Russian actors targeting or compromising are not involved in vote tallying." An assessment based on observations is only as good as those observations and this assessment, in which DHS had only moderate confidence, ¹⁴ suffered from a lack of observable data. As Acting Deputy Undersecretary of Homeland Security for National Protection and Programs Directorate, Jeannette Manfra, testified at the Committee's June 21, 2017, hearing, DHS did not conduct any forensic analysis of voting machines.
- (U) DHS's prepared testimony at that hearing included the statement that it is "likely that cyber manipulation of U.S. election systems intended to change the outcome of a national election would be detected." The language of this assessment raises questions, however, about DHS's ability to identify cyber manipulation that could have affected a very close national election, particularly given DHS's acknowledgment of the "possibility that individual or isolated cyber

¹² See, for example, Committee hearing, March 30, 2017.

¹³ Senators' Personal Cybersecurity Working Group Report, submitted by the Senators' Personal Cybersecurity Working Group, November 2018.

¹⁴ Responses to Questions for the Record from Dr. Samuel Liles, Acting Director of Cyber Division, Office of Intelligence and Analysis; and Jeanette Manfra, Acting Deputy Undersecretary, National Protection and Programs Directorate, following Committee hearing, June 21, 2017.

intrusions into U.S. election infrastructure could go undetected, especially at local levels." ¹⁵ Moreover, DHS has acknowledged that its assessment with regard to the detection of outcome-changing cyber manipulation did not apply to state-wide or local elections. ¹⁶

- (U) Assessments about manipulations of voter registration databases are equally hampered by the absence of data. As the Committee acknowledges, it "has limited information on the extent to which state and local election authorities carried out forensic evaluation of registration databases." Assessments about Russian attacks on the administration of elections are also complicated by newly public information about the infiltration of an election technology company. Moreover, as the Special Counsel reported, the GRU sent spear phishing emails to "Florida county officials responsible for administering the 2016 election" which "enabled the GRU to gain access to the network of at least one Florida county government." ¹⁷
- (U) The Committee, in stating that it had found no evidence that vote tallies were altered or that voter registry files were deleted or modified, rightly noted that the Committee's and the IC's insight into this aspect of the 2016 election was limited. I believe that the lack of relevant data precludes attributing any significant weight to the Committee's finding in this area.
- (U) The Committee's investigation into other aspects of Russia's interference in the 2016 election will be included in subsequent chapters. I look forward to reviewing those chapters and hope that outstanding concerns about members' Committee staff access to investigative material, including non-compartmented and unclassified information, will be resolved.

¹⁵ Responses to Questions for the Record from Dr. Samuel Liles, Acting Director of Cyber Division, Office of Intelligence and Analysis; and Jeanette Manfra, Acting Deputy Undersecretary, National Protection and Programs Directorate, following. Committee hearing, June 21, 2017.

¹⁶ Responses to Questions for the Record from Dr. Samuel Liles, Acting Director of Cyber Division, Office of Intelligence and Analysis; and Jeanette Manfra, Acting Deputy Undersecretary, National Protection and Programs Directorate, following. Committee hearing, June 21, 2017.

¹⁷ Report on the Investigation Into Russian Interference In The 2016 Presidential Election, Special Counsel Robert S. Mueller III, March 2019

ADDITIONAL VIEWS OF SENATORS HARRIS, BENNET, AND HEINRICH

- (U) The Russian government's attack on the 2016 election was the product of a deliberate, sustained, and sophisticated campaign to undermine American democracy. Russian military intelligence carried out a hacking operation targeting American political figures and institutions. The Internet Research Agency—an entity with ties to Russian President Vladimir Putin—used social media to sow disinformation and discord among the American electorate. And, as this report makes clear, individuals affiliated with the Russian government launched cyber operations that attempted to access our nation's election infrastructure, in some cases succeeding.
- (U) The Russian objectives were clear: deepen distrust in our political leaders; exploit and widen divisions within American society; undermine confidence in the integrity of our elections; and, ultimately, weaken America's democratic institutions and damage our nation's standing in the world. The Committee did not discover evidence that Russia changed or manipulated vote tallies or voter registration information, however Russian operatives undoubtedly gained familiarity with our election systems and voter registration infrastructure—valuable intelligence that it may seek to exploit in the future.
- (U) The Committee's report does not merely document the wide reach of the Russian operation; the report reveals vulnerabilities in our election infrastructure that we must collectively address. We do not endorse every recommendation in the Committee's report, and we share some of our colleagues' concerns about the vulnerability that we face, particularly at the state level, where counties with limited resources must defend themselves against sophisticated nation-state adversaries. Nevertheless, the report as a whole makes an important contribution to the public's understanding of how Russia interfered in 2016, and underscores the importance of working together to defend against the threat going forward.
- (U) It is critical that state and local policymakers study the report's findings and work to secure election systems by prioritizing cybersecurity, replacing outdated systems and machines, and implementing audits to identify and limit risk. The Intelligence Community and other federal agencies must improve efforts to detect cyberattacks, enhance coordination with state and local officials, and develop strategies to mitigate threats. And, critically, Congress must take up and pass legislation to secure our elections. We must provide states the funding necessary to modernize and maintain election infrastructure, and we must take commonsense steps to safeguard the integrity of the vote, such as requiring paper ballots in all federal elections.
- (U) Our adversaries will persist in their efforts to undermine our shared democratic values. In order to ensure that our democracy endures, it is imperative that we recognize the threat and make the investments necessary to withstand the next attack.

Allied Security Operations Group

Antrim Michigan Forensics Report

REVISED PRELIMINARY SUMMARY, v2

Report Date 12/13/2020

Client:

Bill Bailey

Attorney:

Matthew DePerno

A. WHO WE ARE

- My name is Russell James Ramsland, Jr., and I am a resident of Dallas County, Texas. I hold an MBA from Harvard University, and a political science degree from Duke University. I have worked with the National Aeronautics and Space Administration (NASA) and the Massachusetts Institute of Technology (MIT), among other organizations, and have run businesses all over the world, many of which are highly technical in nature. I have served on technical government panels.
- I am part of the management team of Allied Security Operations Group, LLC, (ASOG). ASOG is a group of globally engaged professionals who come from various disciplines to include Department of Defense, Secret Service, Department of Homeland Security, and the Central Intelligence Agency. It provides a range of security services, but has a particular emphasis on cybersecurity, open source investigation and penetration testing of networks. We employ a wide variety of cyber and cyber forensic analysts. We have patents pending in a variety of applications from novel network security applications to SCADA (Supervisory Control and Data Acquisition) protection and safe browsing solutions for the dark and deep web. For this report, I have relied on these experts and resources.

B. PURPOSE AND PRELIMINARY CONCLUSIONS

- The purpose of this forensic audit is to test the integrity of Dominion Voting System in how it performed in Antrim County, Michigan for the 2020 election.
- 2. We conclude that the Dominion Voting System is intentionally and purposefully designed with inherent errors to create systemic fraud and influence election results. The system intentionally generates an enormously high number of ballot errors. The electronic ballots are then transferred for adjudication. The intentional errors lead to bulk adjudication of ballots with no oversight, no transparency, and no audit trail. This leads to voter or election fraud. Based on our study, we conclude that The Dominion Voting System should not be used in Michigan. We further conclude that the results of Antrim County should not have been certified.

3. The following is a breakdown of the votes tabulated for the 2020 election in Antrim County, showing different dates for the tabulation of the same votes.

Date	Registered Voters	Total Votes Cast	Biden	Trump	Third Party	Write-In	TOTAL VOTES for President
Nov 3	22,082	16,047	7,769	4,509	145	14	12,423
Nov 5	22,082	18,059	7,289	9,783	255	20	17,327
Nov 21	22,082	16,044	5,960	9,748	241	23	15,949

- 4. The Antrim County Clerk and Secretary of State Jocelyn Benson have stated that the election night error (detailed above by the vote "flip" from Trump to Biden, was the result of human error caused by the failure to update the Mancelona Township tabulator prior to election night for a down ballot race. We disagree and conclude that the vote flip occurred because of machine error built into the voting software designed to create error.
- 5. Secretary of State Jocelyn Benson's statement on November 6, 2020 that "[t]the correct results always were and continue to be reflected on the tabulator totals tape" was false.
- 6. The allowable election error rate established by the Federal Election Commission guidelines is of 1 in 250,000 ballots (.0008%). We observed an error rate of 68.05%. This demonstrated a significant and fatal error in security and election integrity.
- 7. The results of the Antrim County 2020 election are not certifiable. This is a result of machine and/or software error, not human error.
- 8. The tabulation log for the forensic examination of the server for Antrim County from December 6, 2020consists of 15,676 individual events, of which 10,667 or 68.05% of the events were recorded errors. These errors resulted in overall tabulation errors or ballots being sent to adjudication. This high error rates proves the Dominion Voting System is flawed and does not meet state or federal election laws.
- 9. These errors occurred after The Antrim County Clerk provided a re-provisioned CF card with uploaded software for the Central Lake Precinct on November 6, 2020. This means the statement by Secretary Benson was false. The Dominion Voting System produced systemic errors and high error rates both prior to the update and after the update; meaning the update (or lack of update) is not the cause of errors.

- 10. In Central Lake Township there were 1,222 ballots **reversed** out of 1,491 total ballots cast, resulting in an 81.96% rejection rate. All reversed ballots are sent to adjudication for a decision by election personnel.
- 11. It is critical to understand that the Dominion system classifies ballots into two categories, 1) normal ballots and 2) adjudicated ballots. Ballots sent to adjudication can be altered by administrators, and adjudication files can be moved between different Results Tally and Reporting (RTR) terminals with no audit trail of which administrator actually adjudicates (i.e. votes) the ballot batch. This demonstrated a significant and fatal error in security and election integrity because it provides no meaningful observation of the adjudication process or audit trail of which administrator actually adjudicated the ballots.
- 12. A staggering number of votes required adjudication. This was a 2020 issue not seen in previous election cycles still stored on the server. This is caused by intentional errors in the system. The intentional errors lead to bulk adjudication of ballots with no oversight, no transparency or audit trail. Our examination of the server logs indicates that this high error rate was incongruent with patterns from previous years. The statement attributing these issues to human error is not consistent with the forensic evaluation, which points more correctly to systemic machine and/or software errors. The systemic errors are intentionally designed to create errors in order to push a high volume of ballots to bulk adjudication.
- 13. The linked video demonstrates how to cheat at adjudication:

https://mobile.twitter.com/KanekoaTheGreat/status/1336888454538428418

- 14. Antrim County failed to properly update its system. A purposeful lack of providing basic computer security updates in the system software and hardware demonstrates incompetence, gross negligence, bad faith, and/or willful non-compliance in providing the fundamental system security required by federal and state law. There is no way this election management system could have passed tests or have been legally certified to conduct the 2020 elections in Michigan under the current laws. According to the National Conference of State Legislatures Michigan requires full compliance with federal standards as determined by a federally accredited voting system laboratory.
- 15. Significantly, the computer system shows vote adjudication logs for prior years; but all adjudication log entries for the 2020 election cycle are missing. The adjudication process is the simplest way to manually manipulate votes. The lack of records prevents any form of audit accountability, and their conspicuous absence is extremely suspicious since the files exist for previous years using the same software. Removal of these files violates state law and prevents a meaningful audit, even if the Secretary wanted to conduct an audit. We must conclude that the 2020 election cycle records have been manually removed.

- 16. Likewise, all server security logs prior to 11:03 pm on November 4, 2020 are missing. This means that all security logs for the day after the election, on election day, and prior to election day are gone. Security logs are very important to an audit trail, forensics, and for detecting advanced persistent threats and outside attacks, especially on systems with outdated system files. These logs would contain domain controls, authentication failures, error codes, times users logged on and off, network connections to file servers between file accesses, internet connections, times, and data transfers. Other server logs before November 4, 2020 are present; therefore, there is no reasonable explanation for the security logs to be missing.
- 17. On November 21, 2020, an unauthorized user unsuccessfully attempted to zero out election results. This demonstrates additional tampering with data.
- 18. The Election Event Designer Log shows that Dominion ImageCast Precinct Cards were programmed with new ballot programming on 10/23/2020 and then again after the election on 11/05/2020. These system changes affect how ballots are read and tabulated, and our examination demonstrated a significant change in voter results using the two different programs. In accordance with the Help America Vote Act, this violates the 90-day Safe Harbor Period which prohibits changes to election systems, registries, hardware/software updates without undergoing re-certification. According to the National Conference of State Legislatures Michigan requires full compliance with federal standards as determined by a federally accredited voting system laboratory.
- 19. The only reason to change software after the election would be to obfuscate evidence of fraud and/or to correct program errors that would de-certify the election. Our findings show that the Central Lake Township tabulator tape totals were significantly altered by utilizing two different program versions (10/23/2020 and 11/05/2020), both of which were software changes during an election which violates election law, and not just human error associated with the **Dominion Election Management System**. This is clear evidence of software generated movement of votes. The claims made on the **Office of the Secretary of State** website are false.
- The Dominion ImageCast Precinct (ICP) machines have the ability to be connected to the internet (see Image 11). By connecting a network scanner to the ethernet port on the ICP machine and creating Packet Capture logs from the machines we examined show the ability to connect to the network, Application Programming Interface (API) (a data exchange between two different systems) calls and web (http) connections to the Election Management System server. Best practice is to disable the network interface card to avoid connection to the internet. This demonstrated a significant and fatal error in security and election integrity. Because certain files have been deleted, we have not yet found origin or destination; but our research continues.

- 21. Because the intentional high error rate generates large numbers of ballots to be adjudicated by election personnel, we must deduce that bulk adjudication occurred. However, because files and adjudication logs are missing, we have not yet determined where the bulk adjudication occurred or who was responsible for it. Our research continues.
- 22. Research is ongoing. However, based on the preliminary results, we conclude that the errors are so significant that they call into question the integrity and legitimacy of the results in the Antrim County 2020 election to the point that the results are not certifiable. Because the same machines and software are used in 48 other counties in Michigan, this casts doubt on the integrity of the entire election in the state of Michigan.
- 23. DNI Responsibilities: President Obama signed Executive Order on National Critical Infrastructure on 6 January 2017, stating in Section 1. Cybersecurity of Federal Networks, "The Executive Branch operates its information technology (IT) on behalf of the American people. The President will hold heads of executive departments and agencies (agency heads) accountable for managing cybersecurity risk to their enterprises. In addition, because risk management decisions made by agency heads can affect the risk to the executive branch as a whole, and to national security, it is also the policy of the United States to manage cybersecurity risk as an executive branch enterprise." President Obama's EO further stated, effective immediately, each agency head shall use The Framework for Improving Critical Infrastructure Cybersecurity (the Framework) developed by the National Institute of Standards and Technology." Support to Critical Infrastructure at Greatest Risk. The Secretary of Homeland Security, in coordination with the Secretary of Defense, the Attorney General, the Director of National Intelligence, the Director of the Federal Bureau of Investigation, the heads of appropriate sector-specific agencies, as defined in Presidential Policy Directive 21 of February 12, 2013 (Critical Infrastructure Security and Resilience) (sector-specific agencies), and all other appropriate agency heads, as identified by the Secretary of Homeland Security, shall: (i) identify authorities and capabilities that agencies could employ to support the cybersecurity efforts of critical infrastructure entities identified pursuant to section 9 of Executive Order 13636 of February 12, 2013 (Improving Critical Infrastructure Cybersecurity), to be at greatest risk of attacks that could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security (section 9 entities);

This is a national security imperative. In July 2018, President Trump strengthened President Obama's Executive Order to include requirements to ensure US election systems, processes, and its people were not manipulated by foreign meddling, either through electronic or systemic manipulation, social media, or physical changes made in hardware, software, or supporting systems. The 2018 Executive Order. Accordingly, I hereby order:

Section 1. (a) Not later than 45 days after the conclusion of a United States election, the Director of National Intelligence, in consultation with the heads of any other appropriate executive departments and agencies (agencies), shall conduct an assessment of any information indicating that a foreign government, or any person acting as an agent of or on behalf of a foreign government, has acted with the intent or purpose of interfering in that election. The assessment shall identify, to the maximum extent ascertainable, the nature of any foreign interference and any methods employed to execute it, the persons involved, and the foreign government or governments that authorized, directed, sponsored, or supported it. The Director of National Intelligence shall deliver this assessment and appropriate supporting information to the President, the Secretary of State, the Secretary of the Treasury, the Secretary of Defense, the Attorney General, and the Secretary of Homeland Security.

We recommend that an independent group should be empaneled to determine the extent of the adjudication errors throughout the State of Michigan. This is a national security issue.

Michigan resident Gustavo Delfino, a former professor of mathematics in 24. Venezuela and alumni of University of Michigan, offered a compelling affidavit [Exhibit 2] recognizing the inherent vulnerabilities in the SmartMatic electronic voting machines (software which was since incorporated into Dominion Voting Systems) during the 2004 national referendum in Venezuela (see attached declaration). After 4 years of research and 3 years of undergoing intensive peer review, Professor Delfino's paper was published in the highly respected "Statistical Science" journal, November 2011 issue (Volume 26, Number 4) with title "Analysis of the 2004 Venezuela Referendum: The Official Results Versus the Petition Signatures." The intensive study used multiple mathematical approaches to ascertain the voting results found in the 2004 Venezuelan referendum. Delfino and his research partners discovered not only the algorithm used to manipulate the results, but also the precise location in the election processing sequence where vulnerability in machine processing would provide such an opportunity. According to Prof Delfino, the magnitude of the difference between the official and the true result in Venezuela estimated at 1,370,000 votes. Our investigation into the error rates and results of the Antrim County voting tally reflect the same tactics, which have also been reported in other Michigan counties as well. This demonstrates a national security issue.

C. PROCESS

We visited Antrim County twice: November 27, 2020 and December 6, 2020.

On November 27, 2020, we visited Central Lake Township, Star Township, and Mancelona Township. We examined the Dominion Voting Systems tabulators and tabulator roles.

On December 6, 2020, we visited the Antrim County Clerk's office. We inspected and performed forensic duplication of the following:

- 1. Antrim County Election Management Server running Dominion Democracy Suite 5.5.3-002;
- Compact Flash cards used by the local precincts in their Dominion ImageCast Precinct;
- USB memory sticks used by the Dominion VAT (Voter Assist Terminals); and
- 4. USB memory sticks used for the Poll Book.

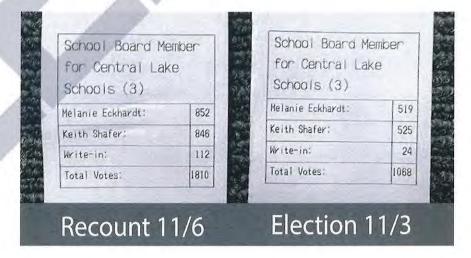
Dominion voting system is a Canadian owned company with global subsidiaries. It is owned by Staple Street Capital which is in turn owned by UBS Securities LLC, of which 3 out of their 7 board members are Chinese nationals. The Dominion software is licensed from Smartmatic which is a Venezuelan owned and controlled company. Dominion Server locations have been determined to be in Serbia, Canada, the US, Spain and Germany.

D. CENTRAL LAKE TOWNSHIP

- On November 27, 2020, part of our forensics team visited the Central Lake Township in Michigan to inspect the **Dominion ImageCast Precint** for possible hardware issues on behalf of a local lawsuit filed by Michigan attorney Matthew DePerno on behalf of William Bailey. In our conversations with the clerk of **Central Lake Township** Ms. Judith L. Kosloski, she presented to us "two separate paper totals tape" from Tabulator ID 2.
 - One dated "Poll Opened Nov. 03/2020 06:38:48" (Roll 1);
 - Another dated "Poll Opened Nov. 06/2020 09:21:58" (Roll 2).
- We were then told by Ms. Kosloski that on November 5, 2020, Ms. Kosloski was notified by Connie Wing of the County Clerk's Office and asked to bring the tabulator and ballots to the County Clerk's office for re-tabulation. They ran the ballots and printed "Roll 2". She noticed a difference in the votes and brought it up to the clerk, but canvasing still occurred, and her objections were not addressed.
- Our team analyzed both rolls and compared the results. Roll 1 had 1,494 total votes and Roll 2 had 1,491 votes (Roll 2 had 3 less ballots because 3 ballots were damaged in the process.)
- 4. "Statement of Votes Cast from Antrim" shows that only **1,491** votes were counted, and the **3** ballots that were damaged were not entered into final results.

- 5. Ms. Kosloski stated that she and her assistant manually refilled out the three ballots, curing them, and ran them through the ballot counting system but the final numbers do not reflect the inclusion of those 3 damaged ballots.
- 6. This is the most preliminary report of serious election fraud indicators. In comparing the numbers on both rolls, we estimate 1,474 votes changed across the two rolls, between the first and the second time the exact same ballots were run through the County Clerk's vote counting machine which is almost the same number of voters that voted in total.
 - 742 votes were added to School Board Member for Central Lake Schools (3)
 - 657 votes were removed from School Board Member for Ellsworth Schools (2)
 - 7 votes were added to the total for State Proposal 20-1 (1) and out of those there were 611 votes moved between the Yes and No Categories.
- 7. There were incremental changes throughout the rolls with some significant adjustments between the 2 rolls that were reviewed. This demonstrates conclusively that votes can be and were changed during the second machine count after the software update. That should be impossible especially at such a high percentage to total votes cast.
- 8. For the School Board Member for Central Lake Schools (3) [Image 1] there were 742 votes added to this vote total. Since multiple people were elected, this did not change the result of both candidates being elected, but one does see a change in who had most votes. If it were a single-person election this would have changed the outcome and demonstrates conclusively that votes can be and were changed during the second machine counting. That should be impossible.

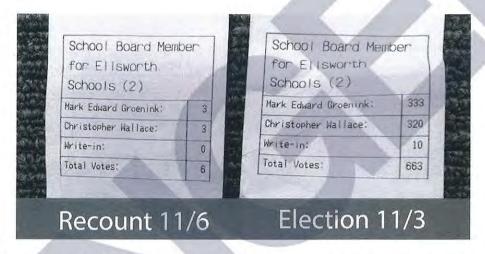
[Image 1]:



- 9. For the School Board Member for Ellsworth Schools (2) [Image 2]
 - Shows 657 votes being removed from this election.
 - In this case, only **3** people who were eligible to vote actually voted. Since there were **2** votes allowed for each voter to cast.
 - The recount correctly shows 6 votes.

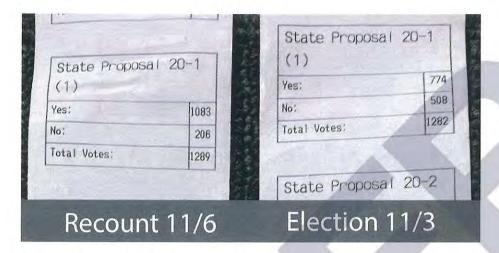
But on election night, there was a major calculation issue:

[Image 2]:



- 10. In **State Proposal 20-1 (1)**, [Image 3] there is a major change in votes in this category.
 - There were 774 votes for YES during the election, to 1,083 votes for YES on the recount a change of 309 votes.
 - 7 votes were added to the total for State Proposal 20-1 (1) out of those there were 611 votes moved between the Yes and No Categories.

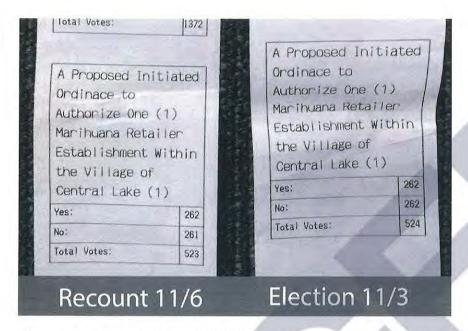
[Image 3]:



- 11. **State Proposal 20-1 (1)** is a fairly technical and complicated proposed amendment to the Michigan Constitution to change the disposition and allowable uses of future revenue generated from oil and gas bonuses, rentals and royalties from state-owned land. Information about the proposal: https://crcmich.org/publications/statewide-ballot-proposal-20-1-michigan-natural-resources-trust-fund
- 12. A Proposed Initiated Ordinance to Authorize One (1) Marihuana (sic) Retailer Establishment Within the Village of Central Lake (1). [Image 4]
 - On election night, it was a tie vote.
 - Then, on the rerun of ballots 3 ballots were destroyed, but only one vote changed on the totals to allow the proposal to pass.

When 3 ballots were not counted and programming change on the tabulator was installed the proposal passed with 1 vote being removed from the No vote.

[Image 4]:



- 13. On Sunday December 6, 2020, our forensics team visited the Antrim County Clerk. There were two USB memory sticks used, one contained the software package used to tabulate election results on November 3, 2020, and the other was programmed on November 6, 2020 with a different software package which yielded significantly different voting outcomes. The election data package is used by the **Dominion Democracy Suite** software & election management system software to upload programming information onto the Compact Flash Cards for the **Dominion ImageCast Precinct** to enable it to calculate ballot totals.
- 14. This software programming should be standard across all voting machines systems for the duration of the entire election if accurate tabulation is the expected outcome as required by US Election Law. This intentional difference in software programming is a design feature to alter election outcomes.
- 15. The election day outcomes were calculated using the original software programming on November 3, 2020. On November 5, 2020 the township clerk was asked to re-run the Central Lake Township ballots and was given no explanation for this unusual request. On November 6, 2020 the Antrim County Clerk, Sheryl Guy issued the second version of software to re-run the same Central Lake Township ballots and oversaw the process. This resulted in greater than a 60% change in voting results, inexplicably impacting every single election contest in a township with less than 1500 voters. These errors far exceed the ballot error rate standard of 1 in 250,000 ballots (.0008%) as required by federal election law.
 - The original election programming files are last dated 09/25/2020 1:24pm
 - The updated election data package files are last dated 10/22/2020 10:27 am.

- As the tabulator tape totals prove, there were large numbers of votes switched from the November 3, 2020 tape to the November 6, 2020 tape. This was solely based on using different software versions of the operating program to calculate votes, not tabulate votes. This is evidenced by using same the Dominion System with two different software program versions contained on the two different USB Memory Devices.
- 17. The Help America Vote Act, Safe Harbor provides a 90-day period prior to elections where no changes can be made to election systems. To make changes would require recertification of the entire system for use in the election. The Dominion User Guide prescribes the proper procedure to test machines with test ballots to compare the results to validate machine functionality to determine if the **Dominion ImageCast Precinct** was programmed correctly. If this occurred a ballot misconfiguration would have been identified. Once the software was updated to the 10/22/2020 software the test ballots should have been re-run to validate the vote totals to confirm the machine was configured correctly.
- 18. The November 6, 2020 note from The Office of the Secretary of State Jocelyn Benson states: "The correct results always were and continue to be reflected on the tabulator totals tape and on the ballots themselves. Even if the error in the reported unofficial results had not been quickly noticed, it would have been identified during the county canvass. Boards of County Canvassers, which are composed of 2 Democrats and 2 Republicans, review the printed totals tape from each tabulator during the canvass to verify the reported vote totals are correct."
 - Source: https://www.michigan.gov/sos/0,4670,7-127-1640_9150-544676--,00.html
- 19. The Secretary of State Jocelyn Benson's statement is false. Our findings show that the tabulator tape totals were significantly altered by utilization of two different program versions, and not just the Dominion Election Management System. This is the opposite of the claim that the Office of the Secretary of State made on its website. The fact that these significant errors were not caught in ballot testing and not caught by the local county clerk shows that there are major inherent built-in vulnerabilities and process flaws in the Dominion Election Management System, and that other townships/precincts and the entire election have been affected.
- 20. On Sunday December 6, 2020, our forensics team visited the Antrim County Clerk office to perform forensic duplication of the **Antrim County Election**Management Server running Dominion Democracy Suite 5.5.3-002.
- 21. Forensic copies of the Compact Flash cards used by the local precincts in their Dominion ImageCast Precinct were inspected, USB memory sticks used by the Dominion VAT (Voter Assist Terminals) and the USB memory sticks used for the Poll Book were forensically duplicated.

22. We have been told that the ballot design and configuration for the **Dominion ImageCast Precinct** and VAT were provided by **ElectionSource.com** which is which is owned by MC&E, Inc of Grand Rapids, MI.

E. MANCELONA TOWNSHIP

- 1. In Mancelona township, problems with software versions were also known to have been present. Mancelona elections officials understood that ballot processing issued were not accurate and used the second version of software to process votes on 4 November, again an election de-certifying event, as no changes to the election system are authorized by law in the 90 days preceding elections without re-certification.
- Once the 10/22/2020 software update was performed on the Dominion ImageCast Precinct the test ballot process should have been performed to validate the programming. There is no indication that this procedure was performed.

F. ANTRIM COUNTY CLERK'S OFFICE

1. Pursuant to a court ordered inspection, we participated in an onsite collection effort at the Antrim County Clerk's office on December 6, 2020. [Image 5]:



Among other items forensically collected, the Antrim County Election Management Server (EMS) with Democracy Suite was forensically collected. [Images 6 and 7].





The EMS (Election Management Server) was a:

Dell Precision Tower 3420.

Service Tag: 6NB0KH2

The EMS contained 2 hard drives in a RAID-1 configuration. That is the 2 drives redundantly stored the same information and the server could continue to operate if either of the 2 hard drives failed. The EMS was booted via the Linux Boot USB memory sticks and both hard drives were forensically imaged.

At the onset of the collection process we observed that the initial program thumb drive was not secured in the vault with the CF cards and other thumbdrives. We watched as the County employees, including Clerk Sheryl Guy searched throughout the office for the missing thumb drive. Eventually they found the missing thumb drive in an unsecured and unlocked desk drawer along with multiple other random thumb drives. This demonstrated a significant and fatal error in security and election integrity.

G. FORENSIC COLLECTION

We used a built for purpose Linux Boot USB memory stick to boot the EMS in a forensically sound mode. We then used Ewfacquire to make a forensic image of the 2 independent internal hard drives.

Ewfacquire created an E01 file format forensic image with built-in integrity verification via MD5 hash.

We used Ewfverify to verify the forensic image acquired was a true and accurate copy of the original disk. That was done for both forensic images.

H. ANALYSIS TOOLS

X-Ways Forensics: We used X-Ways Forensics, a commercial Computer Forensic tool, to verify the image was useable and full disk encryption was not in use. In particular we confirmed that Bit locker was not in use on the EMS.

Other tools used: PassMark – OSForensics, Truxton - Forensics, Cellebrite – Physical Analyzer, Blackbag-Blacklight Forensic Software, Microsoft SQL Server Management Studio, Virtual Box, and miscellaneous other tools and scripts.

I. SERVER OVERVIEW AND SUMMARY

- Our initial audit on the computer running the Democracy Suite Software showed that standard computer security best practices were not applied. These minimum-security standards are outlined the 2002 HAVA, and FEC Voting System Standards – it did not even meet the minimum standards required of a government desktop computer.
- 2. The election data software package USB drives (November 2020 election, and November 2020 election updated) are secured with bitlocker encryption software, but they were not stored securely on-site. At the time of our forensic examination, the election data package files were already moved to an unsecure desktop computer and were residing on an unencrypted hard drive. This demonstrated a significant and fatal error in security and election integrity. Key Findings on Desktop and Server Configuration: There were multiple Microsoft security updates as well as Microsoft SQL Server updates which should have been deployed, however there is no evidence that these security patches were ever installed. As described below, many of the software packages were out of date and vulnerable to various methods of attack.
 - a) Computer initial configuration on 10/03/2018 13:08:11:911
 - b) Computer final configuration of server software on 4/10/2019
 - c) Hard Drive not Encrypted at Rest
 - d) Microsoft SQL Server Database not protected with password.
 - e) Democracy Suite Admin Passwords are reused and share passwords.
 - f) Antivirus is 4.5 years outdated
 - g) Windows updates are 3.86 years out of date.
 - h) When computer was last configured on 04/10/2019 the windows updates were 2.11 years out of date.
 - User of computer uses a Super User Account.

- 3. The hard drive was not encrypted at rest which means that if hard drives are removed or initially booted off an external USB drive the files are susceptible to manipulation directly. An attacker is able to mount the hard drive because it is unencrypted, allowing for the manipulation and replacement of any file on the system.
- 4. The Microsoft SQL Server database files were not properly secured to allow modifications of the database files.
- 5. The Democracy Suite Software user account logins and passwords are stored in the unsecured database tables and the multiple Election System Administrator accounts share the same password, which means that there are no audit trails for vote changes, deletions, blank ballot voting, or batch vote alterations or adjudication.
- 6. Antivirus definition is 1666 days old on 12/11/2020. Antrim County updates its system with USB drives. USB drives are the most common vectors for injecting malware into computer systems. The failure to properly update the antivirus definition drastically increases the harm cause by malware from other machines being transmitted to the voting system.
- 7. Windows Server Update Services (WSUS) Offline Update is used to enable updates the computer which is a package of files normally downloaded from the internet but compiled into a program to put on a USB drive to manually update server systems.
- 8. Failure to properly update the voting system demonstrates a significant and fatal error in security and election integrity.
- 9. There are 15 additional updates that should have been installed on the server to adhere to Microsoft Standards to fix known vulnerabilities. For the 4/10/2019 install, the most updated version of the update files would have been 03/13/2019 which is 11.6.1 which is 15 updates newer than 10.9.1

This means the updates installed were 2 years, 1 month, 13 days behind the most current update at the time. This includes security updates and fixes. This demonstrated a significant and fatal error in security and election integrity.

- Wed 04/10/2019 10:34:33.14 Info: Starting WSUS Offline Update (v. 10.9.1)
- Wed 04/10/2019 10:34:33.14 Info: Used path "D:\WSUSOFFLINE1091_2012R2_W10\cmd\" on EMSSERVER (user: EMSADMIN)
- Wed 04/10/2019 10:34:35.55 Info: Medium build date: 03/10/2019

- Found on c:\Windows\wsusofflineupdate.txt
- *WSUS Offline Update (v.10.9.1) was created on 01/29/2017

*WSUS information found here https://download.wsusoffline.net/

10. Super User Administrator account is the primary account used to operate the Dominion Election Management System which is a major security risk. The user logged in has the ability to make major changes to the system and install software which means that there is no oversight to ensure appropriate management controls – i.e. anyone who has access to the shared administrator user names and passwords can make significant changes to the entire voting system. The shared usernames and passwords mean that these changes can be made in an anonymous fashion with no tracking or attribution.

J. ERROR RATES

- We reviewed the Tabulation logs in their entirety for 11/6/2020. The election logs for Antrim County consist of 15,676 total lines or events.
 - Of the 15,676 there were a total of 10,667 critical errors/warnings or a 68.05% error rate.
 - Most of the errors were related to configuration errors that could result in overall tabulation errors or adjudication. These 11/6/2020 tabulation totals were used as the official results.
- 2. For examples, there were 1,222 ballots **reversed** out of 1,491 total ballots cast, thus resulting in an 81.96% rejection rate. Some of which were reversed due to "Ballot's size exceeds maximum expected ballot size".
 - According to the NCSL, Michigan requires testing by a federally accredited laboratory for voting systems. In section 4.1.1 of the Voluntary Voting Systems Guidelines (VVSG) Accuracy Requirements a. All systems shall achieve a report total error rate of no more than one in 125,000.
 - https://www.eac.gov/sites/default/files/eac_assets/1/28/VVSG.1.1.V OL.1.FINAL1.pdf
 - In section 4.1.3.2 Memory Stability of the VVSG it states that Memory devices used to retain election management data shall have demonstrated error free data retention for a period of 22 months.
 - In section 4.1.6.1 Paper-based System Processing Requirements subsection a. of the VVSG it states "The ability of the system to produce and receive electronic signals from the scanning of the ballot, perform logical and numerical operations upon these data, and reproduce the contents of memory when required shall be sufficiently free of error to enable

satisfaction of the system-level accuracy requirement indicated in Subsection 4.1.1."

- These are not human errors; this is definitively related to the software and software configurations resulting in error rates far beyond the thresholds listed in the guidelines.
- 3. A high "error rate" in the election software (in this case 68.05%) reflects an algorithm used that will weight one candidate greater than another (for instance, weight a specific candidate at a 2/3 to approximately 1/3 ratio). In the logs we identified that the RCV or Ranked Choice Voting Algorithm was enabled (see image below from the Dominion manual). This allows the user to apply a weighted numerical value to candidates and change the overall result. The declaration of winners can be done on a basis of points, not votes. [Image 8]:

choice voting results are evaluated on a district per district basis and each district has a set number of points (100). Elimination and declaration of winners is done on basis of points, not votes.



Figure 11-3: RCV Profile screen

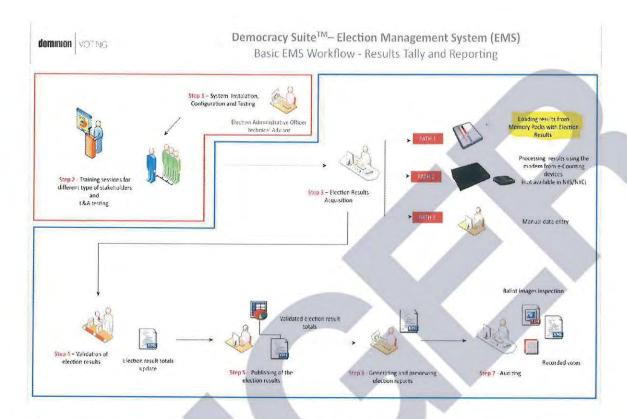
- 4. The Dominion software configuration logs in the Divert Options, shows that all write-in ballots were flagged to be diverted automatically for adjudication. This means that all write-in ballots were sent for "adjudication" by a poll worker or election official to process the ballot based on voter "intent". Adjudication files allow a computer operator to decide to whom to award those votes (or to trash them).
- 5. In the logs all but two of the Override Options were enabled on these machines, thus allowing any operator to change those votes. [Image 9]:



6. In the logs all but two of the Override Options were enabled on these machines, thus allowing any operator to change those votes. This gives the system operators carte blanche to adjudicate ballots, in this case 81.96% of the total cast ballots with no audit trail or oversight. [Image 10]:



7. On 12/8/2020 Microsoft issued 58 security patches across 10+ products, some of which were used for the election software machine, server and programs. Of the 58 security fixes 22, were patches to remote code execution (RCE) vulnerabilities. [Image 11]:



8. We reviewed the Election Management System logs (EmsLogger) in their entirety from 9/19/2020 through 11/21/2020 for the Project: Antrim November 2020. There were configuration errors throughout the set-up, election and tabulation of results. The last error for Central Lake Township, Precinct 1 occurred on 11/21/2020 at 14:35:11 System.Xml.XmlException System.Xml.XmlException: The '' character, hexadecimal value 0x20, cannot be included in a name. Bottom line is that this is a calibration that rejects the vote (see picture below). [Image 12]:



Notably 42 minutes earlier on Nov 21 2020 at 13:53:09 a user attempted to zero out election results. Id:3168 EmsLogger - There is no permission to {0} - Project: User: Thread: 189. This is direct proof of an attempt to tamper with evidence.

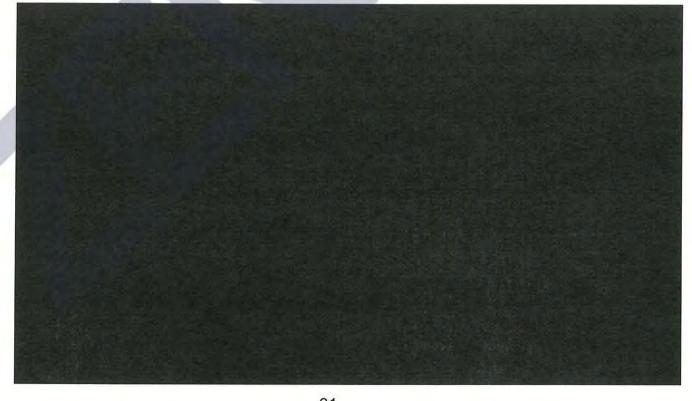


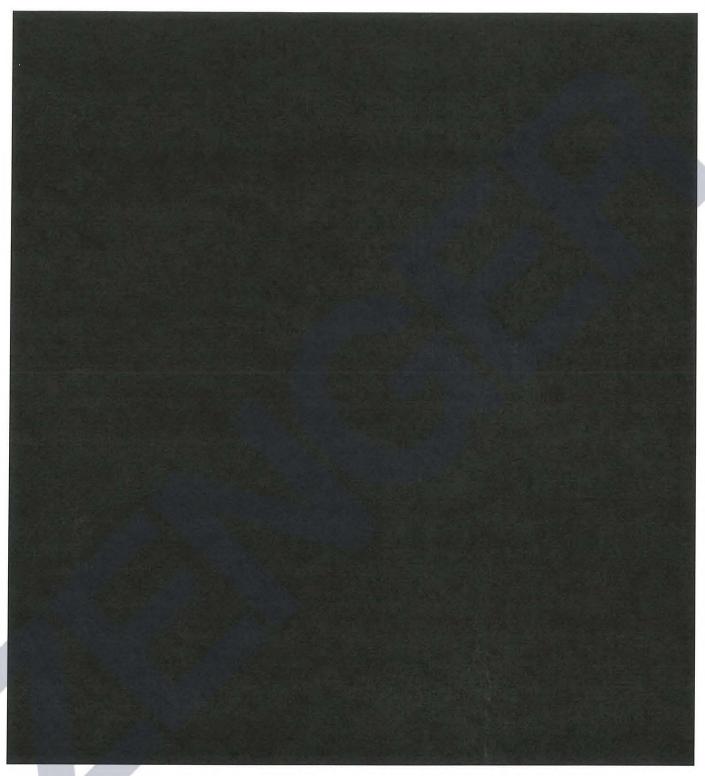
9. The Election Event Designer Log shows that Dominion ImageCast Precinct Cards were programmed with updated new programming on 10/23/2020 and again after the election on 11/05/2020. As previously mentioned, this violates the HAVA safe harbor period.

Source: C:\Program Files\Dominion Voting Systems\Election Event Designer\Log\Info.txt

- Dominion Imagecast Precinct Cards Programmed with 9/25/2020 programming on 09/29/2020, 09/30/2020, and 10/12/2020.
- Dominion Imagecast Precinct Cards Programmed with New Ballot Programming dated 10/22/2020 on 10/23/2020 and after the election on 11/05/2020

Excerpt from 2020-11-05 showing "ProgramMemoryCard" commands.





10. Analysis is ongoing and updated findings will be submitted as soon as possible. A summary of the information collected is provided below.

10|12/07/20 18:52:30| Indexing completed at Mon Dec 7 18:52:30 2020

12|12/07/20 18:52:30| INDEX SUMMARY

12|12/07/20 18:52:30| Files indexed: 159312

12|12/07/20 18:52:30| Files skipped: 64799

12|12/07/20 18:52:30| Files filtered: 0

12|12/07/20 18:52:30| Emails indexed: 0

12|12/07/20 18:52:30| Unique words found: 5325413

12|12/07/20 18:52:30| Variant words found: 3597634

12|12/07/20 18:52:30| Total words found: 239446085

12|12/07/20 18:52:30| Avg. unique words per page: 33.43

12|12/07/20 18:52:30| Avg. words per page: 1503

12|12/07/20 18:52:30| Peak physical memory used: 2949 MB

12|12/07/20 18:52:30| Peak virtual memory used: 8784 MB

12|12/07/20 18:52:30| Errors: 10149

12|12/07/20 18:52:30| Total bytes scanned/downloaded: 1919289906

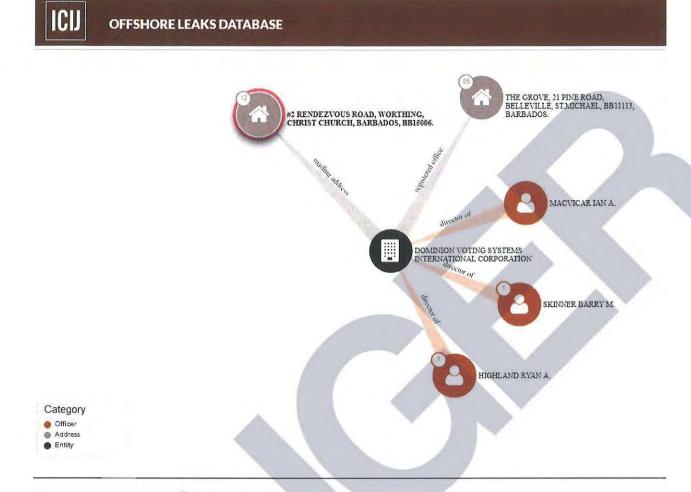
Dated: December 13, 2020

Russell Ramsland

Declaration of	$\times\times\times\times\times\times$	\propto
-----------------------	----------------------------------------	-----------

1.	My name is	, and I am a reside	ent of	🔀. I hold an 🔀	from	
	University, and a	from	University. I am	XXXXX	XXXX	
				****	XXXXX	
		XXXXXX	. Our em	phasis is on digi	tal forensics ar	ıd
	incident response (DFIR) cybersec	urity, analysis of p	ublicly available inform	nation (PAI), pen	etration testing	ğ
	of networks, and problem solving	through operation	ns integration. We use	state-of-the-art t	cools and empl	оу
	a wide variety of cyber and cyber-	forensic analysts.	My colleagues and I are	e currently contr	acted to a cyb	er-
	security and forensics firm that for	cuses on election s	systems.			

- 2. We have examined the various companies, networks, structures, machines, and related global infrastructures directly tied to the 2020 US General Election.
- 3. This is a preliminary report on the various aspects of FOREIGN INTERFERENCE as defined by Executive Order 13848 issued on September 12, 2018.
 - a. Section 8 (f) defines the term "foreign interference," with respect to an election, to include "any covert, fraudulent, deceptive, or unlawful actions or attempted actions of a foreign government, or of any person acting as an agent of or on behalf of a foreign government, undertaken with the purpose or effect of influencing, undermining confidence in, or altering the result or reported result of, the election, or undermining public confidence in election processes or institutions."



https://offshoreleaks.icij.org/nodes/101724285

SMARTMATIC INTERNATIONAL CORPORATION





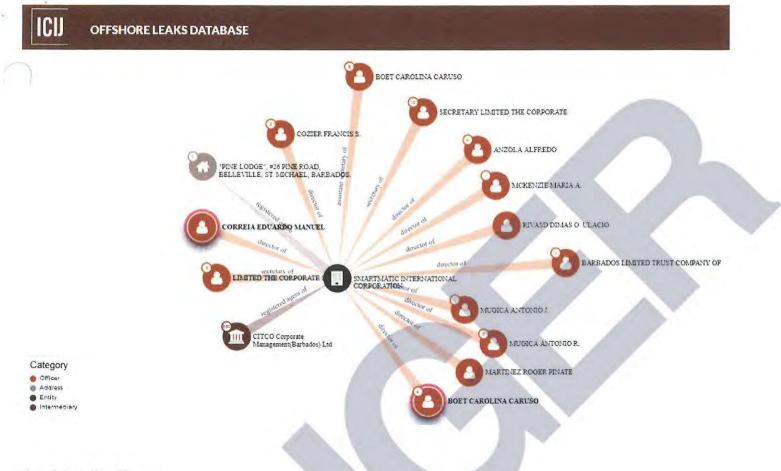
Connected to 1 address

Connected to 13 officers

Connected to 1 intermediary

- incorporated: 29-SEP-2004
- Registered in: Barbados
- ♥ Linked countries: Elarbados

- a Data from: Paradise Papers Barbados corporate registry.
- Barbados corporate registry data is current through 2016
- Q Search in open corporates
- Q Got a tip? Help ICIJ investigate: contact us or leak to us securely

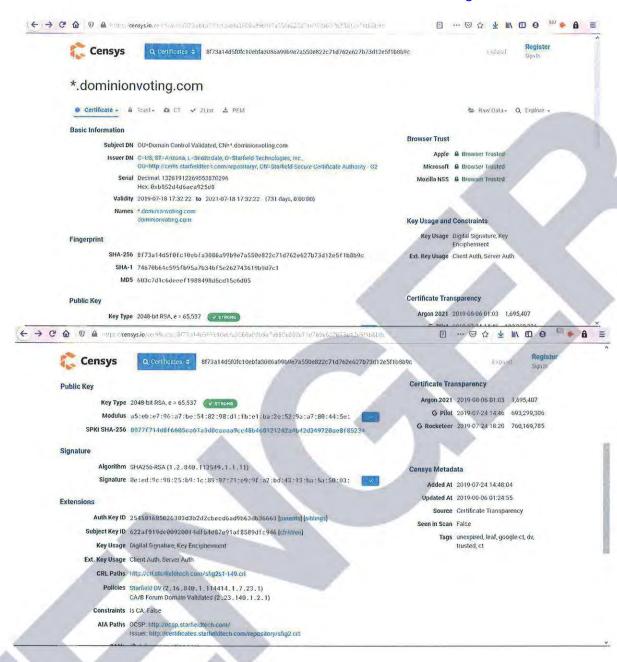


ominion Certificates

25. Dominion can be seen using open-source methodology that the SSL certificates from *.dominionvoting.com were registered on the 24th of July 2019. This SSL certificate were used multiple times from locations ranging from Canada, Serbia, and the United States. These images verify that Dominion systems were connected to foreign systems across the globe. Also seen is that the SSL certificate is used for the email server that was the same for the secure HTTP connections.

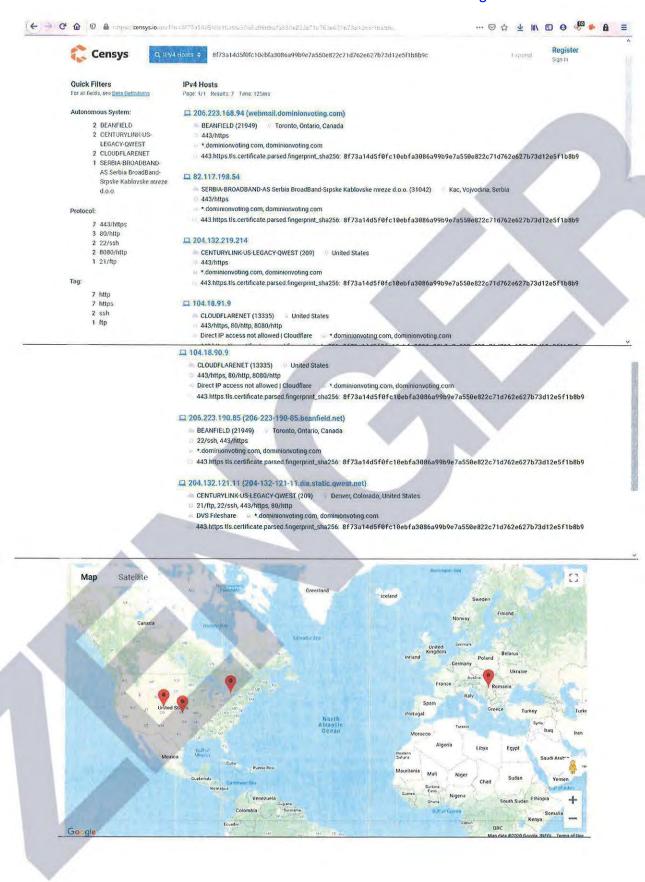
443.https.tls.certificate.parsed.fingerprint_sha256: 8f73a14d5f0fc10ebfa3086a99b9e7a550e822c71d762e627b73d12e5f1b8b9c

Case 1:21-cv-00040 Document 1-113 Filed 01/08/21 Page 125 of 215



al share:

Case 1:21-cv-00040 Document 1-113 Filed 01/08/21 Page 126 of 215



nail ip address:

206.223.168.94

Serbian ip address

82.117.198.54

Dominion site

204.132.219.214

loudflare link

104.18.91.9

Canadian ip address

206.223.190.85

Denver ip address

204.132.121.11

Page: 1/1 Results: 7 Time: 155ms

206.223.168.94 (webmail.dominionvoting.com)

BEANFIELD (21949) Toronto, Ontario, Canada

443/https

*.dominionvoting.com, dominionvoting.com

443.https.tls.certificate.parsed.fingerprint_sha256:

8f73a14d5f0fc10ebfa3086a99b9e7a550e822c71d762e627b73d12e5f1b8b9c

82.117.198.54

SERBIA-BROADBAND-AS Serbia BroadBand-Srpske Kablovske mreze d.o.o. (31042) Kac, Vojvodina, Serbia 443/https

*.dominionvoting.com, dominionvoting.com

443.https.tls.certificate.parsed.fingerprint sha256:

73a14d5f0fc10ebfa3086a99b9e7a550e822c71d762e627b73d12e5f1b8b9c

204.132.219.214

CENTURYLINK-US-LEGACY-QWEST (209) United States

443/https

*.dominionvoting.com, dominionvoting.com

443.https.tls.certificate.parsed.fingerprint_sha256:

8f73a14d5f0fc10ebfa3086a99b9e7a550e822c71d762e627b73d12e5f1b8b9c

104.18.91.9

CLOUDFLARENET (13335) United States

443/https, 80/http, 8080/http

Direct IP access not allowed | Cloudflare *.dominionvoting.com, dominionvoting.com

443.https.tls.certificate.parsed.fingerprint sha256:

8f73a14d5f0fc10ebfa3086a99b9e7a550e822c71d762e627b73d12e5f1b8b9c

104.18.90.9

CLOUDFLARENET (13335) United States

443/https, 80/http, 8080/http

Direct IP access not allowed | Cloudflare *.dominionvoting.com, dominionvoting.com

443.https.tls.certificate.parsed.fingerprint sha256:

8f73a14d5f0fc10ebfa3086a99b9e7a550e822c71d762e627b73d12e5f1b8b9c

206.223.190.85 (206-223-190-85.beanfield.net)

REANFIELD (21949) Toronto, Ontario, Canada

2/ssh, 443/https

*.dominionvoting.com, dominionvoting.com

443.https.tls.certificate.parsed.fingerprint_sha256:
8f73a14d5f0fc10ebfa3086a99b9e7a550e822c71d762e627b73d12e5f1b8b9c
204.132.121.11 (204-132-121-11.dia.static.qwest.net)
ENTURYLINK-US-LEGACY-QWEST (209) Denver, Colorado, United States
21/ftp, 22/ssh, 443/https, 80/http
DVS Fileshare *.dominionvoting.com, dominionvoting.com
443.https.tls.certificate.parsed.fingerprint_sha256:
8f73a14d5f0fc10ebfa3086a99b9e7a550e822c71d762e627b73d12e5f1b8b9c

Supply Chain Concerns

- 28. One in five components used in voting machines are from China-based companies
- 29. On January 6, 2017 DHS Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector.
 - a. This means that election infrastructure becomes a priority within the National Infrastructure

 Protection Plan. It also enables this Department to prioritize our cybersecurity assistance to state

 and local election officials, but only for those who request it. Further, the designation makes clear

 both domestically and internationally that election infrastructure enjoys all the benefits and

 protections of critical infrastructure that the U.S. government has to offer. Finally, a designation

 makes it easier for the federal government to have full and frank discussions with key stakeholders

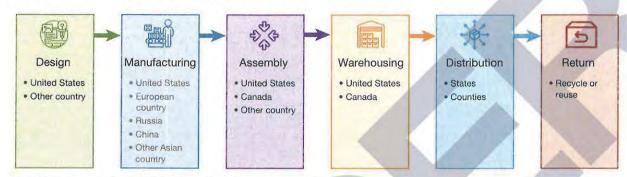
 regarding sensitive vulnerability information.

#: 1687

Case 1:21-cv-00040 Document 1-113 Filed 01/08/21 Page 129 of 215

30. With that in mind, it is incredible that the Election equipment used in the November 3, 2020 election was manufactured in **Russia**, **China** and undisclosed Asian and European Countries (see below).

Phases and Participants in a Supply Chain for Election Equipment for Use in the United States



SOURCE: The countries listed are found in Interos, 2019.

Reference:

https://us-cert.cisa.gov/sites/default/files/2020-10/AA20-304A-Iranian Advanced Persistent Threat Actor Identified Obtaining Voter Registration Data.pdf

https://www.whitehouse.gov/presidential-actions/executive-order-imposing-certain-sanctions-event-foreignhterference-united-states-election/

https://www.jstor.org/stable/resrep26524?seq=13#metadata info tab contents

https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical



De	eclaration of
Pu	rsuant to 28 U.S.C Section 1746, I, make the following declaration.
1.	I am over the age of 21 years and I am under no legal disability, which would prevent me from giving this
	declaration.
2.	
	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
3	Lam a LIS citizen and I recide

4. Whereas the Dominion and Edison Research systems exist in the internet of things, many of their employees and Corporate employees have had their Personally identifiable information, (PII) posted publicly prior to the election and had since deleted information from public websites as well as their company websites. However searching though historic records online, much of their information can be retrieved. The following has to do with key employees and the tied to foreign nations:

Andy Huang, Core Infrastructure Manager of IT at Dominion Voting, previously worked for CCP China Telecom in 1998-2002, has a (jewelry? shell) company called Oriental Net Consulting

Andy Huang, Core Infrastructure Manager of IT at Dominion Voting, previously worked for CCP China Telecom in 1998-2002, has a (jewelry? shell) company called OrientalNet Consulting

Andy Huang currently works as the Core Infrastructure Manager of Information Technology at Dominion Voting Systems. Earlier, he worked at China Telecom for four years between 1998 and 2002. The company is wholly run by the Chinese government. Huang indicates on his LinkedIn that he studied at Dalhousie University in Halifax, Canada.

During his tenure with China Telecom, Huang was tasked with several projects including 'Xiamen Metropolitan-are broadband network', 'Xiamen IDC Project', and 'OA Intranet infrastructure reformation project'. The exact role Huang played in these projects is not known. Huang has also worked with Cisco, a company that contributed significantly to the establishment of the Great Chinese Firewall.

The U.S. Department of Defense has identified China Telecom as having collaborated with the Chinese military for over 20 years. In addition, the U.S. Department of Homeland Security and several other federal agencies had called for a complete ban on China Telecom in April due to national security concerns. Ever since his history with China Telecom became public knowledge, Huang has deleted both China Telecom and Dominion as employers from his LinkedIn profile.

Andy Huang's Chinese pinyin name is Xiaolong Huang as per Canadian incorporation records of OrientalNet Consulting that is indicated in his LinkedIn profile. The addresses and names match when cross-referenced against multiple sources.

OrientalNet Consulting returns as a jewelry trading company on a business listing site, with Andy's name and business details. The address and phone number has changed since.

Searching "OrientalNet Consulting" also returns us "ORIENTALNET CONSULTING LTD. CHINA BRANCH" at another business listing site for Chinese businesses with the below details: "Room 302, Building 4, No.25 Hexiangdong Rd, Xiamen, China (Mainland), Fujian PHONE NUMBER 86-592-8133881 FAX 86-592-5971483 ESTABLISHMENT YEAR 2001

Orientalnet consulting Ltd. China trading branch is a professional manufacturer and exporter specializing in paper products. "

Joyce Zeng is listed as a contact for Orientalnet Consulting Ltd. China Branch. There is no proof that Andy Huang's OrientalNet Consulting is linked to Orientalnet Consulting China Branch, but one thing that is extremely questionable is the jewelry trading company that is linked to him. Was this a shell company?

https://thenationalpulse.com/news/dominion-techie-worked-for-ccp-military-proxy-flagged-by-u-s-govt-for-malicious-cyber-activity/

https://visiontimes.com/2020/11/29/dominion-employee-previously-worked-for-chinese-state-company.html

https://www.can1business.com/company/Active/Orientalnet-Consulting-Ltd

https://www.gmdu.net/corp-276148.html / https://archive.vn/fgioe

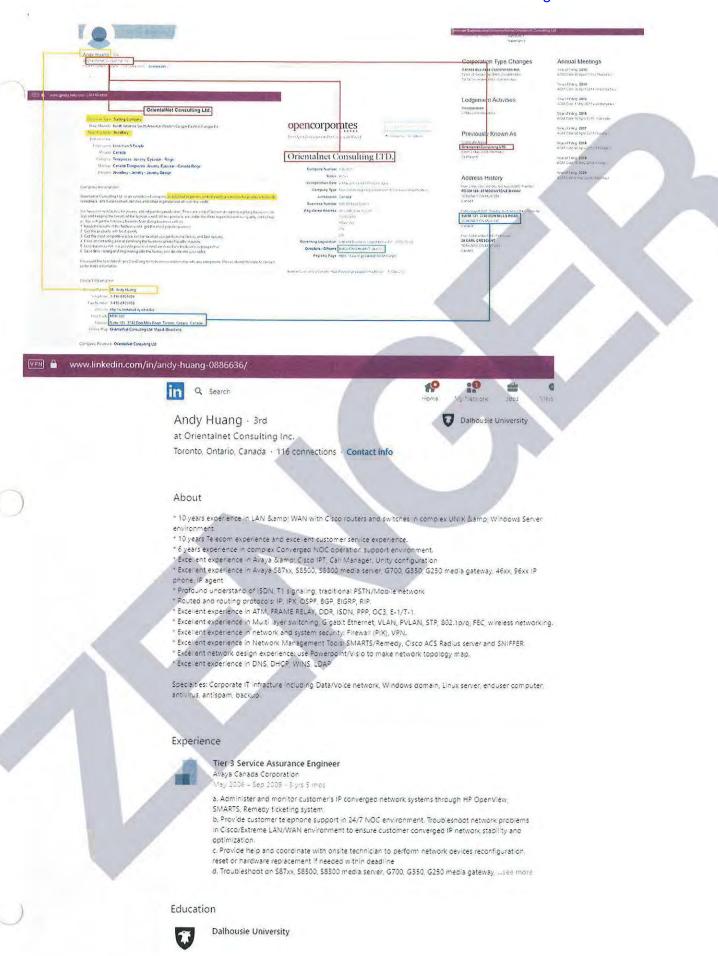
http://www.chinayello.com/company/54513/ORIENTALNET_CONSULTING_LTD_CHINA_BRANCH / https://archive.vn/GYWOY

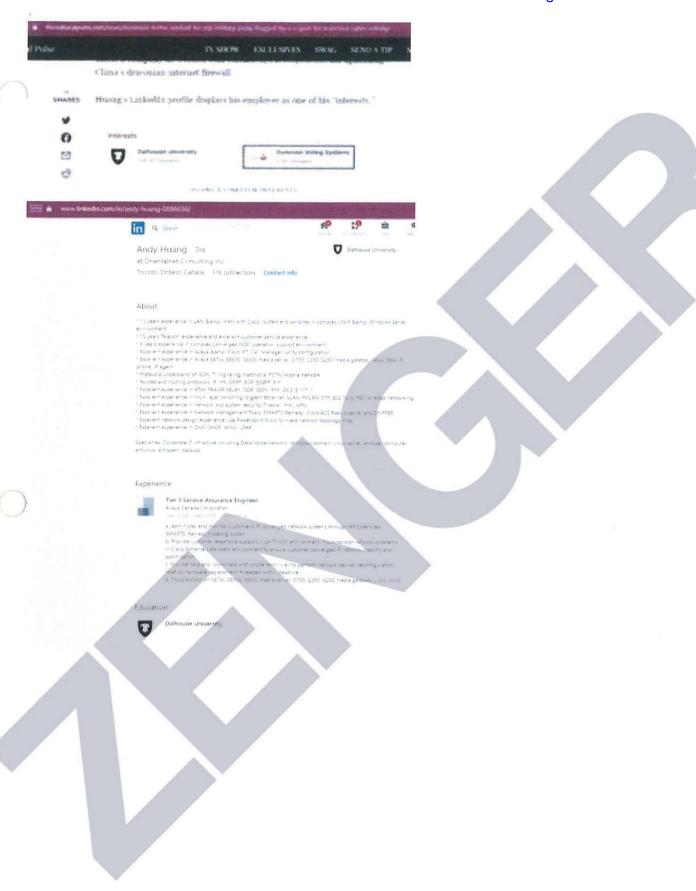
https://www.linkedin.com/in/andy-huang-0886636/

http://www.bizearch.com/company/Orientalnet Consulting Ltd China Branch 24063.htm Andy's LinkedIn prior to him removing a lot of his work history

https://twitter.com/BenKTallmadge/status/1330150320530452487/

Case 1:21-cv-00040 Document 1-113 Filed 01/08/21 Page 132 of 215







Home Trade Leads Product Directory Company Database

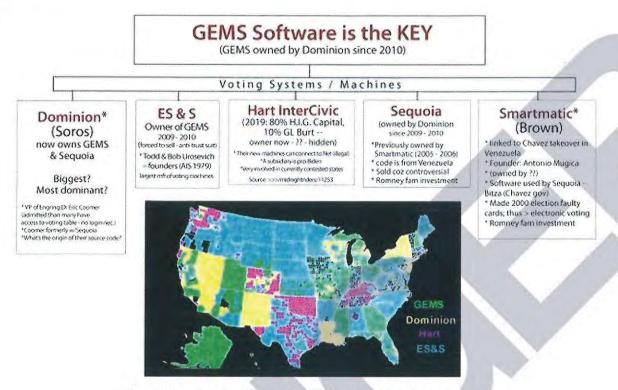
Sign In Join Fre

Orientalnet Consulting Ltd. China Branch





GEMS-Global Election Systems-GEMS central tabulator totals the precinct vote tallies. Firmware (software) is embedded inside the hardware. Dominion acquired, Premier formerly Diebold. Dominion GEM Certificate



Map Source: Fraction Magic - Detailed Vote Rigging Demonstration Beverly Harris - https://www.youtube.com/watch?v=Fob-AGgZn44 - Oct 31, 2016

*Diebold/DESI/Premier owned GEMS until 2009, when it was sold to ES&S, then to Dominion in 2010 (due to an anti-trust suit)

**Smartmatic is not on this map because it has had a non-compete clause with Dominion not to do business within the United States Source: https://www.potteranderson.com/delawarecase-77.html

FINDINGS SO FAR

Voting software & hardware is in the hands of a small gp of companies run by people who have worked together in the industry for years. All have been involved in voter fraud issues. Dominion seems to be the most dominant but all are highly influential & have strong ties to one another and to gov't structures at all levels plus top agencies (e.g., CISA & Homeland Security)

VERSION 4. 11-15-2020

3.1 Software/Firmware

The following software/firmware is required for the execution Dominion Assure 1.3 EAC Modification tests. This includes all supporting software such as operating systems, compilers, assemblers, application software, firmware, any applications used for burning of media, transmission of data or creation/management of databases.

3.1.1 Manufacturer Software/Firmware

The following table details the portions of the Assure 1.3 system that will be exercised in the testing of the modifications.

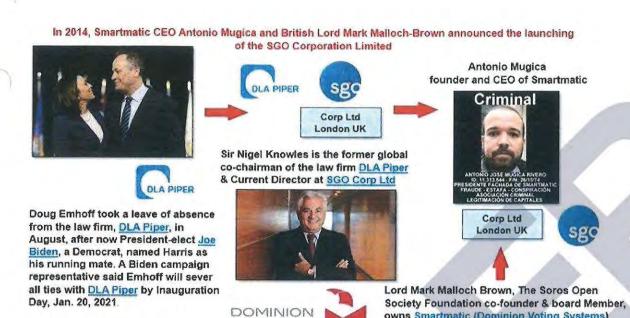
Table 1 - Manufacturer Software/Firmware

Application	Version
GEMS	software version 1.21.6
AV-OS PC	firmware version 1.96.14
AV-OSX	firmware version 1.2.7
AV-TSX DRE	firmware version 4.7.10
AV-TS R6 DRE	firmware version 4.7.10
ABasic script for state of Vermont	in GEMS 1.21.6

3.1.2 Additional Supporting Test Software

No additional supporting test software will be utilized in this certification test campaign.

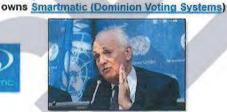
Kamala Harris' husband, Doug Emhoff is partner at DLA Piper. Smartmatic's CEO Antonio Mugica & Lord Mark Malloch-Brown launched SGO Corp whose primary asset is the election technology & voting machine manufacturer. Sir Nigel Knowles, is Co-chairman of DLA Piper & Dir at SGO.



VOTING

Kamala Harris's Husband ????
Connections To Smartmatic &
Dominion Voting Systems...
BY CLOVERCHRONICLE ON NOVEMBER 16, 2020





https://cloverchronicle.com/2020/11/15/kamala-harriss-husband-douglas-empoff-may-have-connections-to-smartmatic-dominion-voting-systems/ https://www.biometricupdate.com/201411/smartmatic-spins-off-new-parent-company-sgo-with-british-ford https://economictimes.indiatimes.com/news/international.world-news/vice-president-elect-kamata-harris-husband-leaves-job-at-powerhouse-law-firmdia-piper/articleshow/79163365.cms

The link Between Dominion, Sequoia, Smartmatic, and the CCP. Sequoia Capital funded Dominion Voting Systems. Neil Shen is the Founder of Sequoia. This is the key to the connection with the Chinese Communist Party (CCP).





Neil Shen is the Founding & Managing Partner of Sequoia Capital China. He is also a co-founder of Ctrip.com (NASDAQ: CTRP) and Home Inns (NASDAQ: HMIN).

A Chinese Bank, HSBC secures the patents pertaining to the U.S. election systems. Dominion Voting Systems entered into a "security agreement" w/ HSBC & received ownership of patents pertaining to intellectual property w/ elections, ballots, systems, cyber & internet capacities.

At this juncture, we are latching on to Sequoia Capital and for good cause. It should be noted here and importantly so, that Sequoia Capital and Sequoia Voting systems are only similar in name. They are not the same entity.

I also recommend taking a quick spin through Sequoia's website by clicking on the above image.

Recall here that Sequoia Capital seeded or funded Dominion Voting Systems and HSBC Toronto acquired from Dominion Voting Systems 18 patents representing the intellectual property of Dominion. Those patents all pertain to direct interfaces with the U.S. election process by means of ballots, systems and machines. Again, see the last article for details here because they are imperative to have.

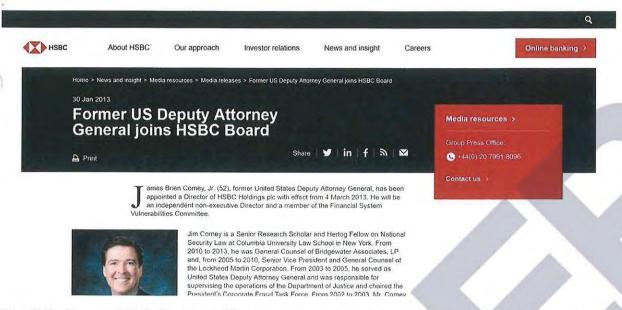
A Toronto-based Chinese bank (HSBC) secures the intellectual patents pertaining to direct access to the U.S. election systems and equipment from Dominion Voting Systems. DVS is seeded by Sequoia Capital, which is affiliated with Cyberbank in the British Virgin Islands. Both Sequoia and HSBC are found in bed together with the China Online Education Group, which follows an established pattern (modus operandi) of directly linking American educators to Chinese foreign nationals for ulterior and nefarious purposes. Immediately pursuant to the stolen 2020 election, HSBC and Sequoia close out their positions on the group and whereby it ties directly to California PERS. California is an immensely corrupt state, its finances are atrocious, Gavin Newsome is the governor and his aunt and fellow resident is Nancy Pelosi. And all of that ties back to the very first article in all of this as it relates to George Soros. And we didn't talk about a mountain's worth of details in between.

At this point, I would refer you to the bank accounts and investment portfolios of Gavin Newsome and Nancy Pelosi. I wonder if either has a trust at Portcullis. I wonder if either has inroads to Cyberbank. I wonder if they hang-out with Shen? What about their connections to HSBC? How do politicians get so filthy rich on their public salaries?

James Comey was appointed to HSBC board of directors. The Massive HSBC Sandal for laundering billions for drug traffickers/arms dealers was covered up when Obama's AG Loretta Lynch struck a deal. Clintons received \$81M Via HSBC Clients. HSBC-Hongkong/Shanghai Bank

https://www.wnd.com/2015/02/emerging-obama-scandal-1st-found-by-wnd-in-2012/





The CCP Captured U.S. by Controlling Sequoia Capital. Smartmatic acquired Sequoia Voting Systems. Smartmatic was co-founded in Venezuela. Venezuela is controlled by the CCP. Smartmatic sold Sequoia Voting Systems to Dominion and continues to use Sequoia's updated software.



The actual controller behind Smartmatic is the former Venezuelan President Chavez. He later transferred management to the current President Maduro. While Venezuela is controlled by the CCP, Maduro is actually the CCP's bagman. In other words, Smartmatic is a company controlled by the CCP, so after its acquisition of Sequoia Voting Systems, the CCP has become the actual controller of the company. After the CCP controlled Sequoia Voting Systems, it developed and updated the voting system software for the CCP. We believe that this voting software has been completely controlled by the CCP since then.

https://en.wikipedia.org/wiki/Smartmatic



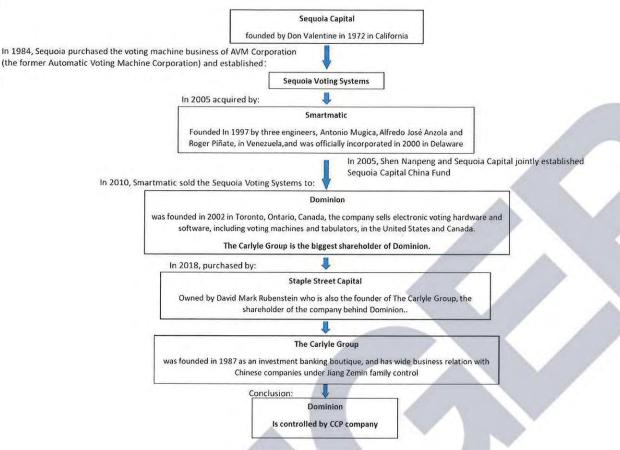
No. 1

Neil Shen

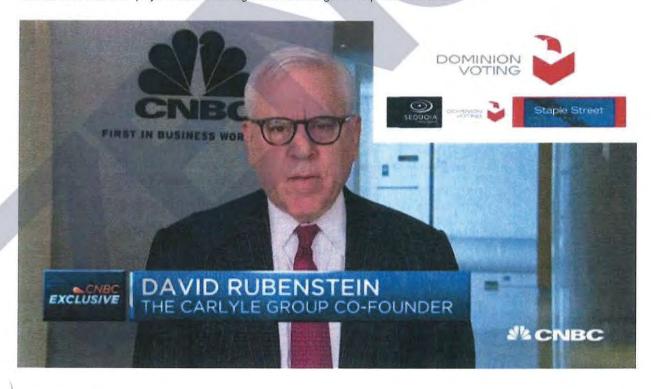
Sequoia Capital China
Founding Partner

The Carlyle Group & The CCP: In 2018, Dominion was acquired by David Rubenstein, founder of The Carlyle Group. The Carlyle Group is the largest global investment company in China. The Carlyle Group ties former George HW Bush & top globalist politicians Worldwide.

CCP Controls Dominion: The controller of Dominion is the Carlyle Group, which is inextricably linked to the CCP. The CCP gained control of Dominion by opening up resource companies to the Carlyle Group. Controlling the votes of Americans, Politicians and the U.S. itself.



We believe this is an exchange of interests between the CCP and Sequoia Capital. Sequoia Capital helps the CCP control Sequoia Voting Systems to realize its ambition to manipulate the American political arena, and the CCP pays it back through the exchange of capital interests.



In 2010, Smartmatic sold Sequoia Voting Systems to Dominion Voting Systems. Dominion continues to use Sequoia's updated software.

HSBC received ownership of patents to intellectual property of elections, ballots, systems, cyber & internet capacities. Patent Agreement

Assignment details for assignee "HSBC BANK CANADA, AS COLLATERAL AGENT"

Assignments (1 total)

0599131

ssignment 1			/
Reel/frame 050500/0236		Execution date	Date recorded
		Sep 25, 2019	Sep 26, 2019
Conveyance SECURITY AGREEMENT			
Assignors		Correspondent	
DOMINION VOTING S	YSTEMS CORPORATION	CHAPMAN & CUTLER	
		1270 AVENUE OF THE ATTN: SOREN SCHWA NEW YORK, NY 10020	
ssignee			
	AS COLLATERAL AGENT		
TH FLOOR, 70 YORK S	TREET		
ORONTO M5J 159 (ANADA			
Properties (18)			
Patent	Publication	Application	PCT
8844813	20130306724	13476836	
8913787	20130301873	13470091	
9202113	20150071501	14539684	
8195505	20050247783	11121997	
9870666	20120232963	13463536	
9710988	20120259680	13525187	
9870667	20120259681	13525208	
7111782	20040238632	10811969	
7422151	20070012767	11526028	

29324281

505692196 09/26/2019

PATENT ASSIGNMENT COVER SHEET

Electronic Version v1.1 Stylesheet Version v1.2

EPAS ID: PAT5739006

SUBMISSION TYPE:		NEW ASSIGNMENT	- 4
NATURE OF CONVEYANCE:		SECURITY AGREEMENT	
CONVEYING PARTY	DATA		1
		Name Execution	on Date
DOMINION VOTING	SYSTEMS	ODDODATION	0
		ORPORATION 09/25/201	9
RECEIVING PARTY	DATA	ANK CANADA, AS COLLATERAL AGENT	9
RECEIVING PARTY	DATA HSBC B		9
RECEIVING PARTY Name:	DATA HSBC B	ANK CANADA, AS COLLATERAL AGENT DOR, 70 YORK STREET	9
RECEIVING PARTY Name: Street Address:	HSBC BA	ANK CANADA, AS COLLATERAL AGENT DOR, 70 YORK STREET	9

PROPERTY NUMBERS Total: 18

Property Type	Number
Patent Number:	8844813
Patent Number:	8913787
Patent Number:	9202113
Patent Number:	8195505
Patent Number:	9870666
Patent Number:	9710988
Patent Number:	9870667
Patent Number:	7111782
Patent Number:	7422151
Patent Number:	D599131
Patent Number:	D521050
Patent Number:	D515619
Patent Number:	D521051
Patent Number:	D537469
Patent Number:	8714450
Patent Number:	8910865
Patent Number:	8864026
Patent Number:	8876002

CORRESPONDENCE DATA

505692196

PATENT REEL: 050500 FRAME: 0236

Fax Number:

Correspondence will be sent to the e-mail address first; if that is unsuccessful, it will be sent

using a fax number, if provided; if that is unsuccessful, it will be sent via US Mail.

Phone:

Email:

212-655-3327

Correspondent Name:

sschwartz@chapman.com CHAPMAN & CUTLER LLP

Address Line 1:

1270 AVENUE OF THE AMERICAS, 30TH FLOOR

Address Line 2:

ATTN: SOREN SCHWARTZ

Address Line 4:

NEW YORK, NEW YORK 10020

SOREN SCHWARTZ

NAME OF SUBMITTER:

/Soren Schwartz/

SIGNATURE:

09/26/2019

DATE SIGNED:

Total Attachments: 5

source=Dominion - Patent Recordation Form#page1.tif

source=Dominion - Patent Recordation Form#page2.tif

source=Dominion - Patent Recordation Form#page3.tif

source=Dominion - Patent Recordation Form#page4.tif

source=Dominion - Patent Recordation Form#page5.tif

Communist People's Republic of China financially captured Collateral of Dominion Voting Systems, Machines & Security Software Applications. Dominion's financial collateral owner is HSBC the Hongkong Shanghai Bank of CHINA-Assigned 18 different Patents.

U.S. Patents & Applications

Title	SERIAL#	FILED DATE	PATENT NO.	ISSUE DATE	STATUS
Electronic Correction of Voter-Marked Paper Ballot	13/476,836	5/21/2012	8,844,813	9/30/2014	Issued
Ballot Adjudication in Voting Systems Utilizing Ballot Images	13/470,091	5/11/2012	8,913,787	12/16/2014	Issued
Ballot Adjudication in Voting Systems Unilizing Ballot Images (continuation of U.S. Patent 8913787)	14/539,684	11/12/2014	9,202,113	12/1/2015	Issued
System, Method and Computer Program for Vote Tabulation with an Electronic Audit Trail	11/121,997	5/5/2005	8,195,505	6/5/2012	Issued
System, Method and Computer Program for Vote Tabulation with an Electronic Audit Trail	13/463,536	5/3/2012	9,870,666	1/16/2018	Issued
System, Method and Computer Program for Vote Tabulation with an Electronic Audit Trail	13/525,187	6/15/2012	9,710,988	7/18/2017	Issued
System, Method and Computer Program for Vote Tabulation with an Electronic Audit Trail	13/525,208	6/15/2012	9,870,667	1/16/2018	Issued
Systems and Methods for Providing Security in a Voting Machine	10/811,969	3/30/2004	7,111,782	9/26/2006	Issued
Systems and Methods for Providing Security in a Voting Machine	11/526,028	9/25/2006	7,422,151	9/9/2008	Issued
Voting Booth	29/324,281	9/10/2008	D599,131	9/1/2009	Issued
Voting Terminal and Stand	29/209.554	7/15/2004	D521,050	5/16/2006	Issued
Pair of Enclosure Doors	29/209,579	7/15/2004	D515,619	2/21/2006	Issued
Voting Terminal	29/209,556	7/15/2004	D521,051	5/16/2006	Issued
Voting Terminal and Keypad	29/254,483	2/23/2006	D537,469	2/27/2007	Issued
Systems and Methods for Transactional Ballot Processing, and Ballot Auditing	13/092,600	4/22/2011	8,714,450	5/6/2014	Issued
Ballot Level Scenrity Features for Optical Scan Voting Machine Capable of Ballot Image Processing, Secure Ballot Printing, and Ballot Layout Authentication and Verification	13/092,599	4/22/2011	8,910,865	12/16/2014	Issued
Ballot Image Processing System and Method for Voting Machines	13/092,606	4/22/2011	8,864,026	10/21/2014	Issued
Systems for Configuring Voting Machines, Docking Device for Voting Machines, Warehouse Support and Asset Fracking of Voting Machines	13/092,604	4/22/2011	8,876,002	11/4/2014	Issued

41""22407 2

Schedule A - Natice of Security Interest in #P

PATENT

REEL: 050500 FRAME: 0241

Ownership of the above-referenced patents has been assigned to Dominion Voting Systems Corporation.

Canadian Patent Application

Title	APPLICATION #	FILED DATE	STATUS
SYSTEM, METHOU AND COMPUTER PROGRAM FOR VOTE TABLE A HON WITH AN ELECTRONIC AUDIT TRAIL	2466466	5/5/2004	Pending

Dominion Voting Systems is listed in the Canadian Patent Office records as the current owner of record for the above-referenced patent application, but this application is to be assigned to Dominion Voting Systems Corporation post-Closing pursuant to the Undertaking

U.S. Registered Trademarks

Trademark	Serial #	File Date	Reg#	Reg Date	Status	Class
3	85407877	Aug-25- 2011	4174339	Jul-17-2012	Registered	35 37 40 41
DOMINION VOTING	85407870	Aug-25- 2011	4174338	Jul-17-2012	Registered	9 35 37 40 4
DEMOCRACY SUITE	85407749	Aug-25- 2011	4153203	Jun-5-2012	Registered	9
IMAGECAST	85407735	Aug-25- 2011	4131899	Apr-24- 2012	Registered	9
AUDITMARK	85407731	Aug-25- 2011	4269144	Jan-1-2013	Registered	9.
ASSURE	78440857	Jun-24-2004	3080674	Apr-11- 2006	Registered	9
AVC ADVANTAGE	73755922	Sep-30-1988	1537309	May-2-1989	Registered	9

Eric Coomer is one of the Inventors of Dominions Voting Security Features. Dominion Voting Systems Patents:

Security, System & Methods:

Assignors: DOMINION VOTING SYSTEMS

Assignee: HSBC

Patent Assignment 050500/0236 SECURITY AGREEMENT

https://assignment.uspto.gov/patent/index.html#/patent/search/resultAssignment?id=50500-236

Case 1:21-cv-00040 Document 1-113 Filed 01/08/21 Page 148 of 215

Patent assignment 050500/0236

SECURITY AGREEMENT 2

 Date recorded
 Real/frame
 Pages

 Sep 26: 2019
 050500/0236
 7

Assignors Execution date
DOMINION VOTING SYSTEMS CORPORATION Sep 25, 2019

Assignee Correspondent
HSBC BANK CANADA, AS COLLATERAL AGENT
4TH FLOOR, 70 YORK STREET 1270 AVENUE OF THE AMERICAS, 30TH FLOOR

TORONTO M5J 1S9 ATTN: SOREN SCHWARTZ
CANADA NEW YORK NY 10020

Properties (18 total)

Patent

1. SYSTEMS AND METHODS FOR PROVIDING SECURITY IN A VOTING MACHINE Inventors: JOHN PAUL HOMEWOOD, THOMAS E, KEELING, PAUL DAVID TERWILLIGER MARC R, LATOUR

7.11.1782

2.004.023.863.2

1.08.11969

Sep 26, 2006

Dec 2, 2004

2. SYSTEM, METHOD AND COMPUTER PROGRAM FOR VOTE TABULATION WITH AN ELECTRONIC AUDIT TRAIL

Application

2. SYSTEM, METHOD AND COMPUTER PROGRAM FOR VOTE TABULATION WITH AN ELECTRONIC AUDIT TRAIL Inventors: JOHN POULOS, JAMES HOOVER, NICK IKONOMAKIS, GORAN OBRADOVIC

8195505 20050247783 11121997 Jun 5, 2012 Nov 10, 2005 May 5, 2005

Publication

3, SYSTEMS AND METHODS FOR PROVIDING SECURITY IN A VOTING MACHINE Inventors: JOHN PAUL HOMEWOOD, THOMAS E, KEELING, PAUL DAVID TERWILLIGER, MARC R, LATOUR

7422151 20070012767 11526028 Sep 9, 2008 Jan 18, 2007 Sep 25, 2006

4. BALLOT LEVEL SECURITY FEATURES: FOR OPTICAL SCANIVOTING MACHINE CAPABLE OF BALLOT IMAGE PROCESSING, SECURE BALLOT PRINTING, AND BALLOT LAYOUT AUTHENTICATION AND VERIFICATION INVENTORS: ERIC COOMER, LARRY KORB, BRIAN GLENN LIERMAN

Eric Coomer is one of the Inventors of Dominions Voting Security Features.

Properties (18)

Patent	Publication	Application	PCT	International registration
8844813	20130306724	13476836		- 4
8913787	20130301873	13470091		
9202113	20150071501	14539684		
8195506	20050247783	11121997		
9870666	20120232963	13463536		
9710988	20120259680	13525187		
9870667	20120259681	13525208		
7111782	20040238632	10811969		Y
7422151	20070012767	11526028	9	
D599131		29324281		

View all

This searchable database contains all recorded Patent Assignment information from August 1980 to the present.

When the USPTO receives relevant information for its assignment database, the USPTO puts the information in the public record and does not verify the validity of the information. Recordation is a ministerial function—the USPTO neither makes a determination of the legality of the transaction nor the right of the submitting party to take the action.

Release 2.0.0 | Release Notes | Send Feedback | Legacy Patent Assignment Search | Legacy Trademark Assignment Search

Assignment details for assignee "HSBC BANK CANADA, AS COLLATERAL AGENT"

Assignments (1 total)

Assignment 1

Reel/frame	Execution date	Date	Pages
050500/0236	Sep 25, 2019	recorded	7
		Sep 26,	
		2019	

Conveyance

SECURITY AGREEMENT

Assignors Correspondent Attorney docket

DOMINION VOTING SYSTEMS CORPORATION

CHAPMAN & CUTLER LLP 1270 AVENUE OF THE AMERICAS, 30TH FLOOR ATTN: SOREN SCHWARTZ NEW YORK, NY 10020

Assignee

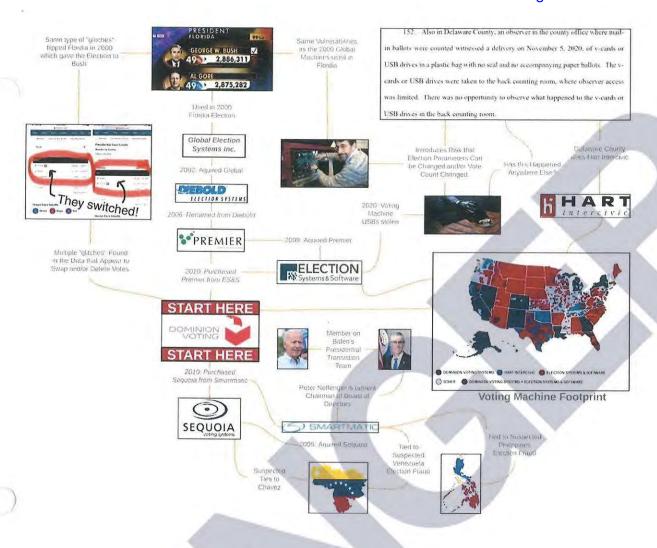
HSBC BANK CANADA, AS COLLATERAL AGENT

4TH FLOOR, 70 YORK STREET

TORONTO M5J 1S9

CANADA

Case 1:21-cv-00040 Document 1-113 Filed 01/08/21 Page 151 of 215



Dominion's parent company Staple Street Capital

Owners of Dominion Voting systems, many of their leadership comes from Cerberus Capital management, from their Vice President to their Managing Director. Cerberus capital owns Remington, Bushmaster and others. This is mentioned because of the effects of the uncertainty during the pandemic and the weapons sales in the United states in regards to their profit for 2020.

Case 1:21-cv-00040 Document 1-113 Filed 01/08/21 Page 152 of 215

Staple Street Capital has 7 current team members, including Senior Associate Daniel Franklin.



Daniel Franklin Senior Associate



Jeffrey D Hyslop Vice President



Andre Ohnona Vice President



Scott Zhu Vice President



Hootan Yaghoobzadeh Managing Director



Stephen D Owens Managing Director & Founder



Dylan Lam Associate

Who owns the Dominion Voting Systems?

July 16, 2018 Dominion Voting Systems ("Dominion Voting") announces that it has been acquired by its management team and Staple Street Capital.

Staple Street Capital is a private equity firm founded in 2009 based in New York. The co-founders Stephen D. Owens and Hootan Yaghoobzadeh are veterans of The Carlyle Group and Cerberus Capital Management, also the Board members of Dominion Voting. The official website of Staple Street Capital has deleted the team introduction.





With staple street capital's ownership of Dominion, Dominion would have been included in the buy out or Staple street when UBS bought them in 2019 for 400 Million Dollars US.

Case 1:21-cv-00317-DCLC-CHS Document 22-7 Filed 01/20/22 Page 153 of 591 PageID

Case 1:21-cv-00040 Document 1-113 Filed 01/08/21 Page 153 of 215

	Exchange Commission has not nec The reader sho	essarily reviewed the informuld not assume that the info	nation in this filing and rmation is accurate and	has not determined if it is accurate complete.	e and complete.	
	UNITED STATES SE	CURITIES AND EXCHAN Washington, D.C. 20549 FORM D	NGE COMMISSION		OMB APPROV	AL 3235-0076
	Notice of	Exempt Offering of Sec	curities		Estimated average burden hours per response:	4.00
. Issuer's Identity					A	
OO(1827586 Name of Issuer STAPLE STREET CAPITAL III, L.P. Jurisdiction of Incorporation/Organization DELAWARE (var of Incorporation/Organization Over Five Years Ago Within Last Five Years (Specify Year) 2020 Yet to Se Formed	Previous Nar	mes ⊠None		Entity Type Corporation X Limited Partnership Limited Liability Company General Partnership Business Trust Other (Specify)		
Principal Place of Business and Contact Info	ormation			1	4	
lame of Issuer TTAPLE STREET CAPITAL III. L.P. Street Address 1 290 AVENUE OF THE AMERICAS, 10TH FLOOR. Sty	State/Province/Country	Street Address 2	4	Ohasa Humbar et legues		
NEW YORK	NEW YORK	10104	,	Phone Number of Issuer (212) 613-3100	- 4	N.Y
. Related Persons						1
S. Related Persons					1	
Last Name OWENS Street Address 1 1250 ATENNE OF THE AMERICAS, 10TH FLOOR City NEW YORK Relationship MExecutive Officer Oriental Fromoter	First Name STEPHEN Street Address 2 State/Produce/Country NEW YORK		Middle Name D ZIP/PostalCode 19104			
Clarification of Response (if Necessary)						
NEW YORK	State/Province/Country NEW YORK		ZIP/PostalCode 10104			
Investment Banking Pharma M Pooled Investment Fund Cither H Hedge Fund Manufactu	NEW YORK Retailing inology Restaurants insurance Technology Is & Physicians Computers councils Telecommunications leabth Care Chemicogy fing Travel					
City KEW YORK Relationship SExecutive Officer Director SPromoter Itarification of Response (if Necessary) I. Industry Group Agriculture	NEW YORK Retailing inology Restaurants insurance Technology Is & Physicians Computers councils Telecommunications leabth Care Chemicogy fing Travel				<u>.</u>	
ENY YORK Relationship Sexecutive Officer Director Promoter relatification of Response (if Necessary) Industry Group Agriculture Health Car Banking & Financial Services Banking Health Car Investment Banking Pharma Medge Fund Manufactur Medge Fund Real Estat Sprivate Equity Fund Real Estat Whether Cardial Eund Constant Fund Constant Fun	NEW YORK Retailing mology Restaurants insurance Technology ts & Physicians Computers ceuticals Talecommunications teatht Care Other Technology ring Tavet s Artines & Airports Estate Artines & Airports Estate Lodging & I	Auroorts Conventions Travel Services			¥.	^
City NEW YORK Relationship Sexecutive Officer Orientor Promoter Distriction of Response (if Necessary) Industry Group	NEW YORK Te Retaining Including Residurants Insurance Technology Is & Physicians Computers Icounicals Talecommunications Is alth Care Cheriology Ing Tavel Artines & Airports Insurance Cherical Cherical Instruction Tourism & Its & Finance Cother Trave Sidential Other Trave	Auroorts Conventions Travel Services			· ·	
Eay New York Relationship Sexecutive Officer Director Promoter Itarification of Response (if Necessary) Industry Group Agriculture Banking & Financial Services Commercial Banking Health Car Insurance Hospital Health Car Professional Epide Monufactur Private Equity Fund Real Estat Nenture Capital Fund Car Other Investinent Fund Car Other Investment Company under the Investment Company and the Insurance Company Act of 1940? Real Estat Ness Services No Other Banking & Financial Services Business Services Energy Coal Mining Electric Utilities Energy Conservation Environmental Services Oil & Gas	NEW YORK Te Retaining Including Residurants Insurance Technology Is & Physicians Computers Icounicals Talecommunications Is alth Care Cheriology Ing Tavel Artines & Airports Insurance Cherical Cherical Instruction Tourism & Its & Finance Cother Trave Sidential Other Trave	Auroorts Conventions Travel Services			¥	

Case 1:21-cv-00040 Document 1-113 Filed 01/08/21 Page 154 of 215

6. Federal Exemption(s) and Exclusion(s) Claimed (select all that ap	ply)		
	X Investment Company Act Sect	ion 3(c)	
По . сомим	X Section 3(c)(1)	Section 3(c)(9)	
Rule 504(b)(1) (not (i), (ii) or (iii)) Rule 504 (b)(1)(i)	=		
Rule 504 (b)(1)(ii)	Section 3(c)(2)	Section 3(c)(10)	
Rule 504 (b)(1)(iii)	Section 3(c)(3)	Section 3(c)(11)	
X Rule 506(b)	Section 3(c)(4)	Section 3(c)(12)	
Rule 506(c)	Section 3(c)(5)	Section 3(c)(13)	
Securities Act Section 4(a)(5)	Section 3(c)(6)	Section 3(c)(14)	
	X Section 3(c)(7)		
7. Type of Filing			
X New Notice Date of First Sale X First Sale Yet to Occur			
Amendment			4
8. Duration of Offering			
Does the Issuer intend this offering to last more than one year?	No		
9. Type(s) of Securities Offered (select all that apply)			
X Equity	Ne	ooled Investment Fund Interests	
Debt		enant-in-Common Securities	
Option, Warrant or Other Right to Acquire Another Security		Ineral Property Securities	
Security to be Acquired Upon Exercise of Option, Warrant or Other Rig		ther (describe)	
10. Business Combination Transaction			
10. Business Combination Transaction		AW	
Is this offering being made in connection with a business combination transact	ion, such as a merger, acquisition or exchange	offer?	K No
Clarification of Response (if Necessary):			
11. Minimum Investment		V III	
20 20 41 20 41 20 41 20 41 20 41 20 41 20 41 20 41 20 41 20 41 20 41 20 41 20 41 20 41 20 41 20 41 20 41 20 41			
Minimum investment accepted from any outside investor \$0 USD			
12. Sales Compensation			
Recipient	Recipient CRD Nun	nber None	
UBS SECURITIES LLC	7654		
(Associated) Broker or Dealer X None	(Associated) Broke	or Dealer CRD Number X None	
None	None		
Street Address 1 1285 AVENUE OF THE AMERICAS	Street Address 2		
City	State/Province/Cour	try	ZIP/Postal Code
NEW YORK	NEW YORK		10019
State(s) of Solicitation (select all that apply) Check "All States" or check individual States	Foreign/non-US		
13. Offering and Sales Amounts			
Total Offering Amount \$400,000,000 USD of Indefinite			
Total Amount Sold \$0 USD			
Total Remaining to be Sold \$400,000,000 USD or Indefinite			
Clarification of Response (if Necessary):			
	Similard matters interests. The Total OO' in A	and Total Barraining to to Cald an array of the	mathetic Towns and its related as 11 to 2
The general partner of the Issuer reserves the right to offer a greater or lesser amount of 14. Investors	numer partner interests, the Total Ottering Amoun	and total Kemaning to be Sold are aggregated together	with the issuer and its related parallel fund
THE HIVE DEVIS	A 21 10 10 10 10 10 10 10 10 10 10 10 10 10		KIND OF THE WAY IN
I Select if securities in the offering have been or may be sold to persons who			

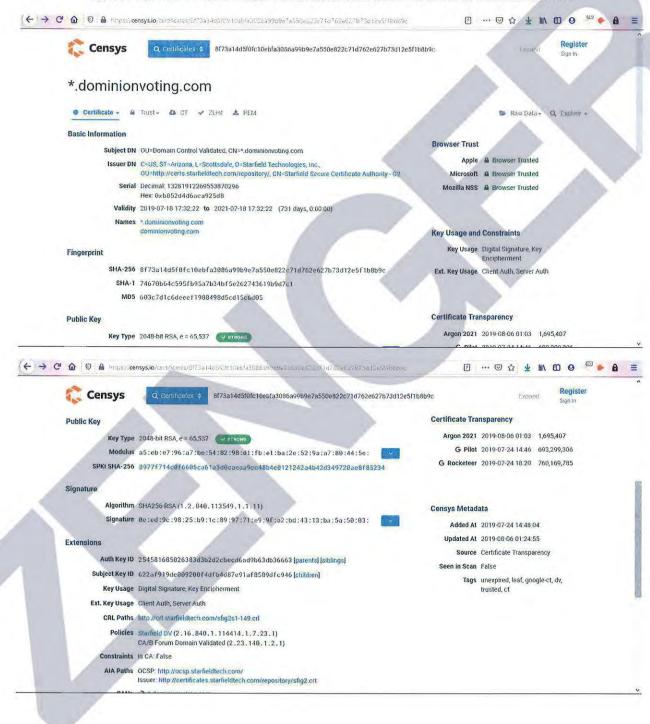
Case 1:21-cv-00040 Document 1-113 Filed 01/08/21 Page 155 of 215

Regardless of whether securities in the of 15. Sales Commissions & Finder's Fees E Provide separately the amounts of sales com Sales Commissions § 0 USD Finders' Fees \$ 0 USD Clarification of Response (if Necessary): Placement agent fees to be paid based upon a fee. 16. Use of Proceeds Provide the amount of the gross proceeds of the amount is unknown, provide an estimate: So USD Clarification of Response (if Necessary):	offering have been or may be sold to persons w Expenses minissions and finders fees expenses, if any. If Estimate Schedule. Such fees are offset dollar-for-dollar again the offering that has been or is proposed to be	the amount of an expenditure is not known, pro	her of such non-accredited investors who already have invested in the offering: the total number of investors who already have invested in the offering: value an estimate and check the box next to the amount.	0
15. Sales Commissions & Finder's Fees E Provide separately the amounts of sales com Sales Commissions \$0 USD Finders' Fees \$0 USD Clarification of Response (if Necessary). Placement agent fees to be paid based upon a fee. 16. Use of Proceeds Provide the amount of the gross proceeds of the amount is unknown, provide an estimate. \$0 USD Clarification of Response (if Necessary). The general partner is estitled to a performance all	Expenses MEstimate Estimate Schedule: Such fees are offset dollar-for-dollar again the offering that has been or is proposed to be and check the box next to the amount.	the amount of an expenditure is not known, pro		0
Provide separately the amounts of sales com Sales Commissions \$0 USD Finders' Fees \$0 USD Clarification of Response (if Necessary): Placement agent fees to be paid based upon a fee. 16. Use of Proceeds Provide the amount of the gross proceeds of the amount is unknown, provide an estimate: So USD Clarification of Response (if Necessary): The general partner is entitled to a performance all	minissions and finders fees expenses, if any, if	nst the management fees payable by the Issuer,	oxide an estimate and check the box next to the amount.	
Sales Commissions \$0 USD Finders' Fees \$0 USD Clarification of Response (if Necessary): Placement agent fees to be paid based upon a fee. 16. Use of Proceeds Provide the amount of the gross proceeds of the amount is unknown, provide an estimate: SO USD Clarification of Response (if Necessary): The general partner is entitled to a performance all	Estimate Substimate Substima	nst the management fees payable by the Issuer,	vide an estimate and check the box next to the amount.	
Finders' Fees \$0 USD Clarification of Response (if Necessary): Placement agent fees to be paid based upon a fee. 16. Use of Proceeds Provide the amount of the gross proceeds of the amount is unknown, provide an estimate: SO USD Clarification of Response (if Necessary): The general partner is entitled to a performance all	Estimate schedule. Such fees are offset dollar-for-dollar again the offering that has been or is proposed to be and check the box next to the amount.	September 1997		
Clarification of Response (if Necessary): Placement agent fees to be paid based upon a fee. 16. Use of Proceeds Provide the amount of the gross proceeds of the amount is unknown, provide an estimate: SO USD Clarification of Response (if Necessary): The general partner is entitled to a performance all	the offering that has been or is proposed to be and check the box next to the amount.	September 1997		
Placement agent fees to be paid based upon a fee- 16. Use of Proceeds Provide the amount of the gross proceeds of the amount is unknown, provide an estimate: So USD Clarification of Response (if Necessary): The general partner is entitled to a performance al	the offering that has been or is proposed to be and check the box next to the amount.	September 1997		
16. Use of Proceeds Provide the amount of the gross proceeds of the amount is unknown, provide an estimate 50 USD Clarification of Response (if Necessary): The general partner is entitled to a performance all	the offering that has been or is proposed to be and check the box next to the amount.	September 1997		
Provide the amount of the gross proceeds of the amount is unknown, provide an estimate So USO Clarification of Response (if Necessary): The general partner is entitled to a performance all	and check the box next to the amount.	used for enuments to any of the servers requi		
the amount is unknown, provide an estimate: 50 USD Clarification of Response (if Necessary): The general partner is entitled to a performance at	and check the box next to the amount.	used for narments to any of the nersons require		7
Clarification of Response (if Necessary): The general partner is entitled to a performance al	X Estimate	used to payments to any of the persons requi	red to be named as executive officers, directors or promoters in respon-	se to Item 3 above.
The general partner is entitled to a performance al				\mathcal{A}
The general partner is entitled to a performance al				-
	allocation. The investment manager is entitled to a m	sanagement fee. The performance allocation and ma	magement fees are fully disclosed in the Issuer's confidential offering materials	
Please verify the information you have er	intered and review the Terms of Submissio	n below before signing and clicking SUBM	IT below to file this notice.	
Terms of Submission	The second secon	in which we do a signify who cheanly boom	To bottom to me and modes.	
In submitting this notice, each issuer named	I above is:			
		nurties described and undergation to funish th	em, upon written request, in the accordance with applicable law, the infi	
offerees.*	in which this notice is ned or the oneining of sec	conces described and undertaking to turnish th	em, upon written request, in the accordance with applicable law, the intro	ormation turnished t
Irrevocably appointing each of the Sec	cretary of the SEC and, the Securities Adminis	trator or other legally designated officer of the S	State <mark>in</mark> which the issuer maintains its principal place of business and a , process or pleading, and further agreeing that such service may be m	any State in which t
For signature, type in the signer's name or ot	ther letters or characters adopted or authorize	d as the signer's signature.		
STAPLE STREET CAPITAL III, L.P.		Name of Singar	Tota	Del
STATLE STREET CAPITAL III, L.F.	Signature /S/HOOTAN YAGHOOBZADEH	Name of Signer	Title MANAGER OF THE GP OF THE JSSUER	
	S/HOOTAN YAGHOOBZADEH	HOOTAN YAGHOOBZADEH	MANAGER OF THE GP OF THE ISSUER	
Persons who respond to the collection	s/HOOTAN YAGHOOBZADEH on of information contained in this for	HOOTAN YAGHOOBZADEH m are not required to respond unless	MANAGER OF THE GP OF THE ISSUER the form displays a currently valid OMB number.	Dat 2020-10-6
Persons who respond to the collection	s/HOOTAN YAGHOOBZADEH on of information contained in this for	HOOTAN YAGHOOBZADEH m are not required to respond unless	MANAGER OF THE GP OF THE ISSUER	2020-10-4

De	eclaration of
Pu	rsuant to 28 U.S.C Section 1746, I, make the following declaration.
1.	I am over the age of 21 years and I am under no legal disability, which would prevent me from giving this declaration.
2.	
2	
٥.	I am a US citizen and I reside at in the United States of America.

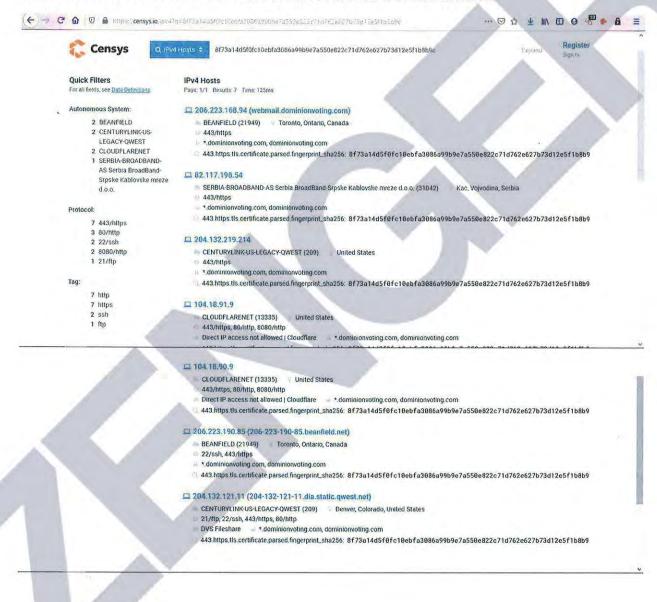
4. It can be seen using open source methodology that the SSL certificates from *.dominionvoting.com were registered on the 24th of July 2019. This SSL certificate were used multiple times from locations ranging from Canada, Serbia, and the United States. These images verify that Dominion systems were connected to foreign systems across the globe. Also seen is that the SSL certificate is used for the email server that was the same for the secure HTTP connections.

443.https.tls.certificate.parsed.fingerprint_sha256: 8f73a14d5f0fc10ebfa3086a99b9e7a550e822c71d762e627b73d12e5f1b8b9c



All share:

443.https.tls.certificate.parsed.fingerprint_sha256: 8f73a14d5f0fc10ebfa3086a99b9e7a550e822c71d762e627b73d12e5f1b8b9





Email ip address

206.223.168.94

Serbian ip address

82.117.198.54

Dominion site

204.132.219.214

Cloudflare link

104.18.91.9

Canadian ip address

206.223.190.85

Denver ip address

204.132.121.11

Page: 1/1 Results: 7 Time: 155ms

206.223.168.94 (webmail.dominionvoting.com)

BEANFIELD (21949) Toronto, Ontario, Canada

443/https

*.dominionvoting.com, dominionvoting.com

443.https.tls.certificate.parsed.fingerprint sha256:

8f73a14d5f0fc10ebfa3086a99b9e7a550e822c71d762e627b73d12e5f1b8b9c

82.117.198.54

SERBIA-BROADBAND-AS Serbia BroadBand-Srpske Kablovske mreze d.o.o. (31042) Kac,

Vojvodina, Serbia

443/https

*.dominionvoting.com, dominionvoting.com

443.https.tls.certificate.parsed.fingerprint sha256:

8f73a14d5f0fc10ebfa3086a99b9e7a550e822c71d762e627b73d12e5f1b8b9c

204.132.219.214

CENTURYLINK-US-LEGACY-QWEST (209) United States

443/https

*.dominionvoting.com, dominionvoting.com

443.https.tls.certificate.parsed.fingerprint sha256:

8f73a14d5f0fc10ebfa3086a99b9e7a550e822c71d762e627b73d12e5f1b8b9c

104.18.91.9

CLOUDFLARENET (13335) United States

443/https, 80/http, 8080/http

Direct IP access not allowed | Cloudflare *.dominionvoting.com, dominionvoting.com

443.https.tls.certificate.parsed.fingerprint sha256:

8f73a14d5f0fc10ebfa3086a99b9e7a550e822c71d762e627b73d12e5f1b8b9c

104.18.90.9

CLOUDFLARENET (13335) United States

443/https, 80/http, 8080/http

Direct IP access not allowed | Cloudflare *.dominionvoting.com, dominionvoting.com

443.https.tls.certificate.parsed.fingerprint sha256:

8f73a14d5f0fc10ebfa3086a99b9e7a550e822c71d762e627b73d12e5f1b8b9c

206.223.190.85 (206-223-190-85, beanfield, net)

BEANFIELD (21949) Toronto, Ontario, Canada

22/ssh, 443/https

*.dominionvoting.com, dominionvoting.com

443.https.tls.certificate.parsed.fingerprint sha256:

8f73a14d5f0fc10ebfa3086a99b9e7a550e822c71d762e627b73d12e5f1b8b9c

204.132.121.11 (204-132-121-11.dia.static.qwest.net)

CENTURYLINK-US-LEGACY-QWEST (209) Denver, Colorado, United States

21/ftp, 22/ssh, 443/https, 80/http

DVS Fileshare *.dominionvoting.com, dominionvoting.com

443.https.tls.certificate.parsed.fingerprint_sha256:

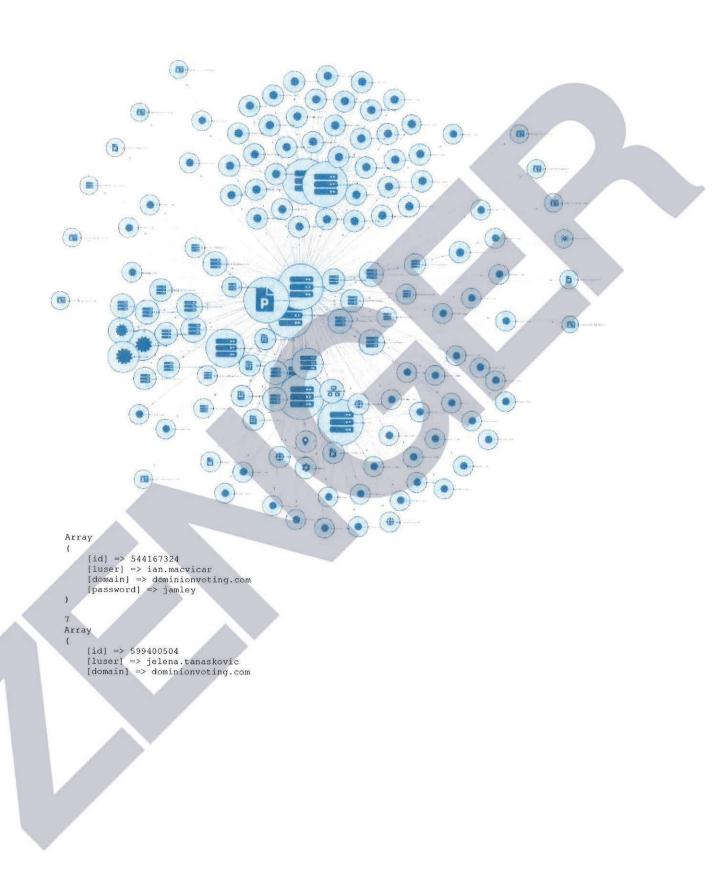
8f73a14d5f0fc10ebfa3086a99b9e7a550e822c71d762e627b73d12e5f1b8b9c

I declare under penalty of perjury that the forgoing is tru knowledge. Executed this December 16, 2020.

Foreign Ties and Vulnerabilities

De	eclaration of
Pu	ursuant to 28 U.S.C Section 1746, I, make the following declaration.
1.	I am over the age of 21 years and I am under no legal disability, which would prevent me
	from giving this declaration.
2.	
3.	I am a US citizen and I reside in the United States of America.

- 4. Whereas the Dominion and Edison Research systems exist in the internet of things, and whereas this makes the network connections between the Dominion, Edison Research and related network nodes available for scanning,
- 5. And whereas Edison Research's primary job is to report the tabulation of the count of the ballot information as received from the tabulation software, to provide to Decision HQ for election results,
- 6. And whereas Spiderfoot and Robtex are industry standard digital forensic tools for evaluation network security and infrastructure, these tools were used to conduct public security scans of the aforementioned Dominion and Edison Research systems,
- A public network scan of Dominionvoting.com on 2020-11-08 revealed the following interrelationships and revealed 13 unencrypted passwords for dominion employees, and 75 hashed passwords available in TOR nodes:



8. The same public scan also showed a direct connection to the group in Belgrade as highlighted below:



8 results shown.

IP numbers of the name servers

2400:cb00:2049:1::adf5:3bb3

2606:4700:50::adf5:3aad 2803:f800:50::6ca2:c0ad 2803:f800:50::6ca2:c1b3 2a06:98c1:50::ac40:20ad

108.162.192.173

108.162.192.173

Subdomains/Hostnames

Domains or hostnames one step under this dom

barracuda.dominionvoting.com

belgrade.dominionvoting.com webmail.dominionvoting.com

www.dominionvoting.com

4 results shown.

9. A cursory search on LinkedIn of "dominion voting" on 11/19/2020 confirms the numerous employees in Serbia:



Vukašin Đorđević · 3rd

Software Developer at Dominion Voting Systems Serbia



Edvan Sabanovic · 3rd

Senior Full-stack Web Developer

Belgrade, Serbia

Past; Senior Web Developer at Dominion Voting Systems

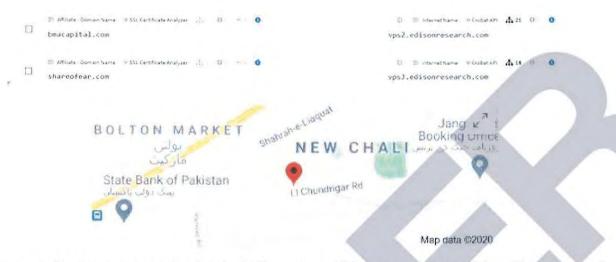
10. An additional search of Edison Research on 2020-11-08 showed that Edison Research has an Iranian server seen here:



Inputting the Iranian IP into Robtex confirms the direct connection into the "edisonresearch" host from the perspective of the Iranian domain also. This means that it is not possible that the connection was a unidirectional reference.

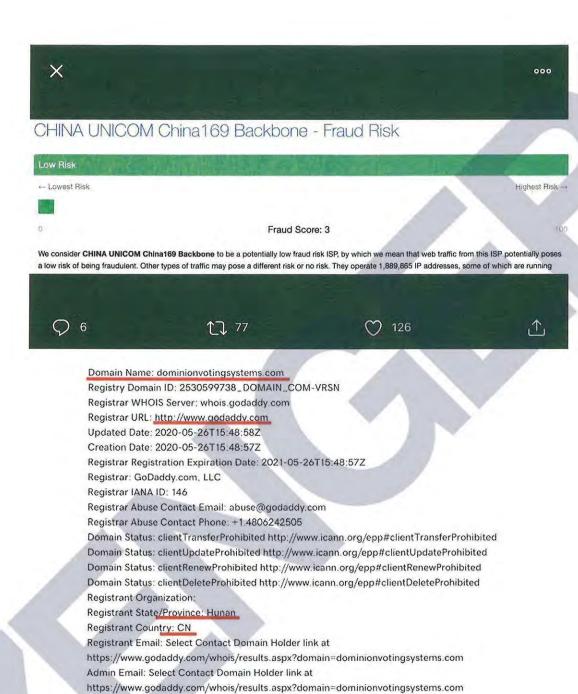


A deeper search of the ownership of Edison Research "edisonresearch.com" shows a connection to BMA Capital Management, where shareofear.com and bmacapital.com are both connected to edisonresearch.com via a VPS or Virtual Private Server, as denoted by the "vps" at the start of the internet name:



There are also many more examples, including access of the network from China. The records of China accessing the server are reliable.





https://www.godaddy.com/whois/results.aspx?domain=dominionvotingsystems.com

Tech Email: Select Contact Domain Holder link at

Name Server: NS1.DNS.COM Name Server: NS2.DNS.COM

DNSSEC: unsigned



11. BMA Capital Management is known as a company that provides Iran access to capital markets with direct links publicly discoverable on LinkedIn (found via google on 11/19/2020):

www.linkedin.com > muhammad-talha-a0759660

Muhammad Talha - BMA Capital Management Limited

Manager, Money Market & Fixed Income at BMA Capital Management Limited. BMA Capital ... Manager-FMR at Pak Iran Joint Investment Company. Pakistan.

Pakistan · Manager, Money Market & Fixed Income · BMA Capital Management Limited

The same Robtex search confirms the Iranian address is tied to the server in the Netherlands, which correlates to known OSINT of Iranian use of the Netherlands as a remote server (See Advanced Persistent Threats: APT33 and APT34):



12. A search of the indivisible.org network showed a subdomain which evidences the existence of scorecard software in use as part of the Indivisible (formerly ACORN) political group for Obama:



- 13. Each of the tabulation software companies have their own central reporting "affiliate". Edison Research is the affiliate for Dominion.
- 14. Beanfield.com out of Canada shows the connections via co-hosting related sites, including dvscorp.com:

This domain redirects to beanfield.com



This Dominion partner domain "dvscorp" also includes an auto discovery feature, where new innetwork devices automatically connect to the system. The following diagram shows some of the dvscorp.com mappings, which mimic the infrastructure for Dominion:





The above diagram shows how these domains also show the connection to Iran and other places, including the following Chinese domain, highlighted below:



- 15. The auto discovery feature allows programmers to access any system while it is connected to the internet once it's a part of the constellation of devices (see original Spiderfoot graph).
- 16. Dominion Voting Systems Corporation in 2019 sold a number of their patents to China (via HSBC Bank in Canada):

Assignment details for assignee "HSBC BANK CANADA, AS COLLATERAL AGENT"

Assignments (1 total)

Assignment 1

Execution date	Date	Pages
Sep 25, 2019	recorded	7
- 60	Sep 26,	
	2019	1
		Sep 25, 2019 Sep 26,

Conveyance

SECURITY AGREEMENT

Assignors Correspondent Attorney docket

DOMINION VOTING SYSTEMS CORPORATION CHAPMAN & CUTLER LLP
1270 AVENUE OF THE

AMERICAS, 30TH FLOOR ATTN: SOREN SCHWARTZ NEW YORK, NY 10020

Assignee

HSBC BANK CANADA, AS COLLATERAL AGENT

4TH FLOOR, 70 YORK STREET

TORONTO M5J 1S9

CANADA

Properties (18)

	Patent	Publication	Application	PCT	International
	ratent	Fublication	Application		registration
	8844813	20130306724	13476836		
	8913787	20130301873	13470091		1
	9202113	20150071501	14539684	4	
	8195505	20050247783	11121997		
	9870666	20120232963	13463536		
	9710988	20120259680	13525187	V	
	9870667	20120259681	13525208		
	7111782	20040238632	10811969		
4	7422151	20070012767	11526028		
	D599131		29324281		

View all

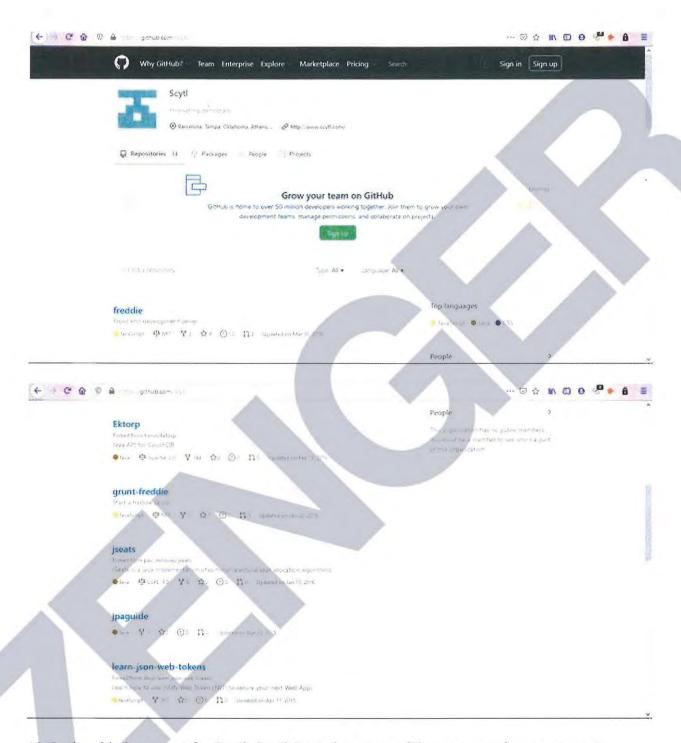
This searchable database contains all recorded Patent Assignment information from August 1980 to the present.

When the USPTO receives relevant information for its assignment database, the USPTO puts the information in the public record and does not verify the validity of the information. Recordation is a ministerial function—the USPTO neither makes a determination of the legality of the transaction nor the right of the submitting party to take the action.

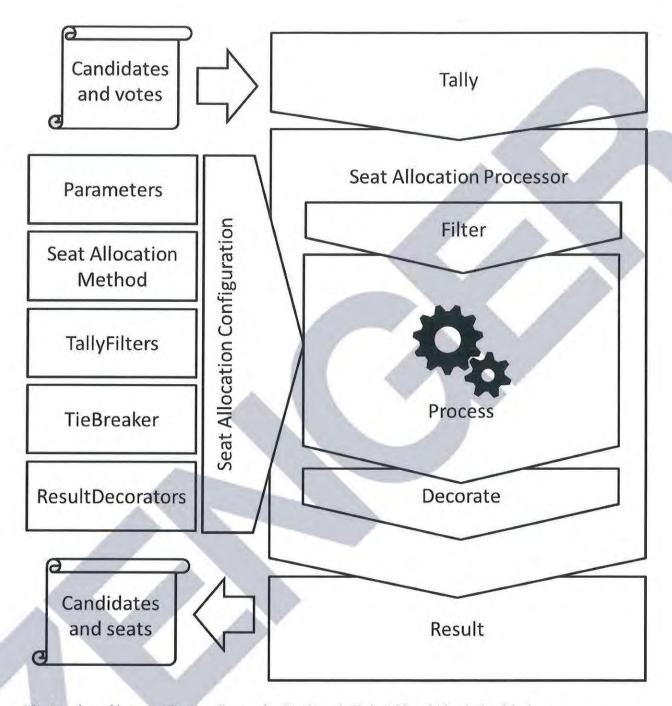
Release 2.0.0 | Release Notes | Send Feedback | Legacy Patent Assignment Search | Legacy Trademark Assignment Search Of particular interest is a section of the document showing aspects of the nature of the patents dealing with authentication:



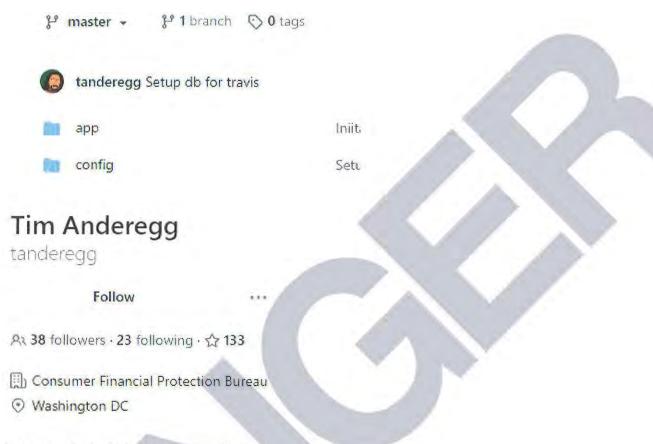
17. Smartmatic creates the backbone (like the cloud). CTCL is responsible for the security within the election system.



18. In the github account for Scytl, Scytl Jseats has some of the programming necessary to support a much broader set of election types, including a decorator process where the data is smoothed, see the following diagram provided in their source code:



19. A point of interest for the Center for Tech and Civic Life within their github page (https://github.com/ctcl) is that one of the programmers for Edison Research holds a government position. The Bipcoop repo shows tanderegg as one of the developers, and he works at the Consumer Financial Protection Bureau:



20. As seen in included document titled

"AA20-304A-

Iranian_Advanced_Persistent_Threat_Actor_Identified_Obtaining_Voter_Registration_Data "that was authored by the Cybersecurity & Infrastructure Security Agency (CISA) with a Product ID of AA20-304A on a specified date of October 30, 2020, CISA and the FBI reports that Iranian APT teams were seen using ACUTENIX, a website scanning software, to find vulnerabilities within Election company websites, confirmed to be used by the Iranian APT teams buy seized cloud storage that I had personally captured and reported to higher authorities. These scanning behaviors showed that foreign agents of aggressor nations had access to US voter lists, and had done so recently.

21. In my professional opinion, this affidavit presents unambiguous evidence that Dominion Voter Systems and Edison Research have been accessible and were certainly compromised by rogue actors, such as Iran and China. By using servers and employees connected with rogue actors and hostile foreign influences combined with numerous easily discoverable leaked credentials, these organizations neglectfully allowed foreign adversaries to access data

and intentionally provided access to their infrastructure in order to monitor and manipulate elections, including the most recent one in 2020. This represents a complete failure of their duty to provide basic cyber security. This is not a technological issue, but rather a governance and basic security issue: if it is not corrected, future elections in the United States and beyond will not be secure and citizens will not have confidence in the results.

I declare under penalty of perjury that the forgo knowledge. Executed this December 16th, 2020



Case 1:21-cv-00040 Document 1-113 Filed 01/08/21 Page 179 of 215

Smartmatic SSL Certificate

De	eclaration of
Pu	rsuant to 28 U.S.C Section 1746, I, make the following declaration.
1.	I am over the age of 21 years and I am under no legal disability, which would prevent me from giving this
	declaration.
2.	
3.	I am a US citizen and I reside at in the United States of America.

4. Researching Smartmatic's website and reading their public manuals about the reuse of SSL certificate's, I started to investigate Smartmatic's SSL certificates. Upon searching their website is currently behind Cloudflare yet using the same SSL certificate it made it easy to locate where Smartmatic's website was located. Smartmatic's website is in the Philippine's on their Election commission's server (Comelec.gov.ph).

Case 1:21-cv-00040 Document 1-113 Filed 01/08/21 Page 180 of 215







Quick Filters

For all fields, see Data Definitions

Protocol:

1 25/smtp

Tag:

1 smtp

Websites

Page: 1/1 Results: 1 Time: 18ms

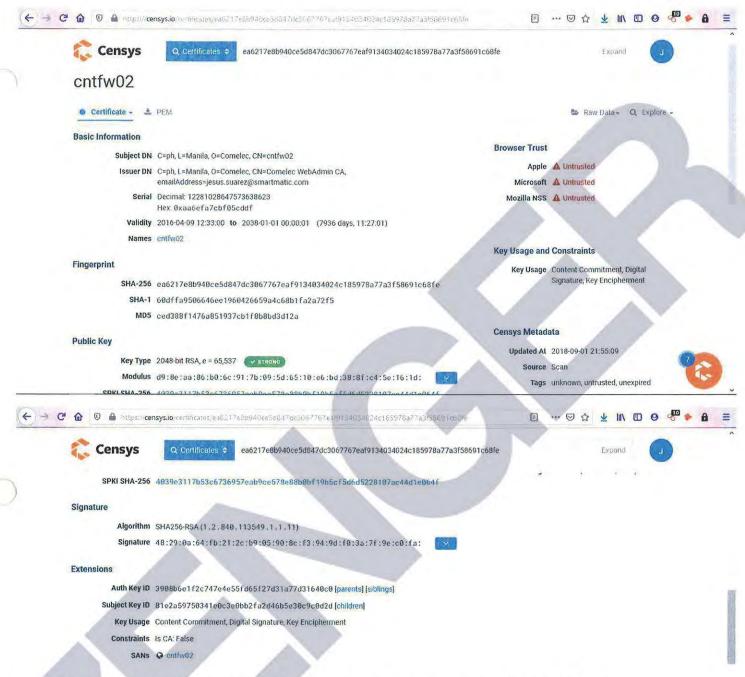
* comelec.gov.ph (172.67.165.108)

117,344 25/smtp



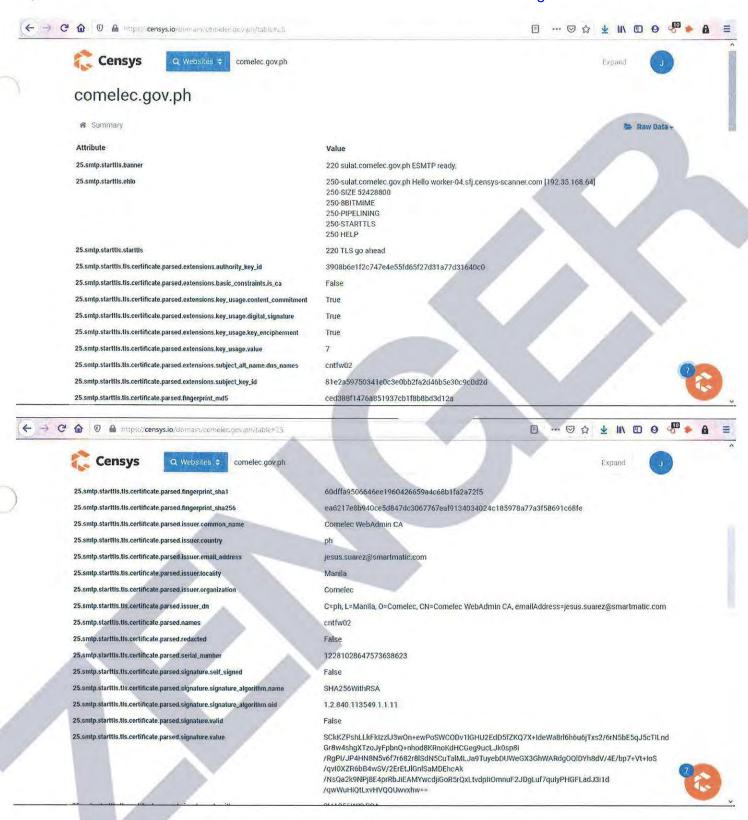
C=ph, L=Manila, O=Comelec, CN=Comelec WebAdmin CA, emailAddress=jesus.suarez@smartmatic.com

Case 1:21-cv-00040 Document 1-113 Filed 01/08/21 Page 182 of 215

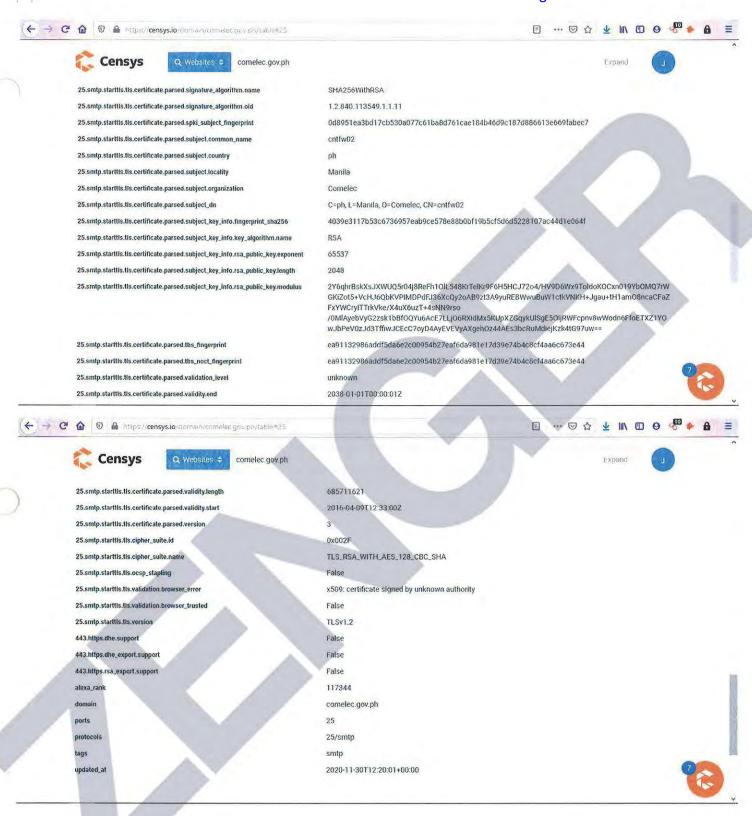


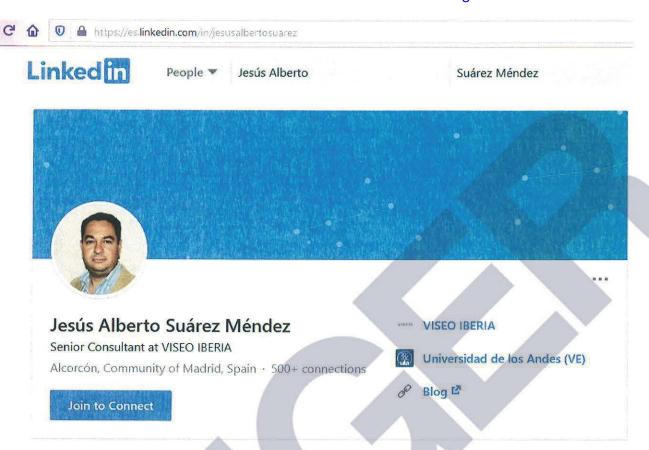
5. As can be seen in the images above the SSL certificate used was registered by the email address jesus.suarez@smartmatic.com on the 9th of April 2016.

Case 1:21-cv-00040 Document 1-113 Filed 01/08/21 Page 183 of 215



Case 1:21-cv-00040 Document 1-113 Filed 01/08/21 Page 184 of 215





About

DevOps SysAdmin and Information Security Professional with more than 20 years of experience. Specialized in Security and IT Management, IT Risk Assessment and Management, IT architecture, automatized deployments on Linux environment and cloud using DevOps tools. Very interested in





People *

Jesús Alberto

Suárez Méndez



Master Information Security Specialist

Smartmatic

Aug 2008 - Mar 2017 · 8 years 8 months

Caracas, Venezuela

Design, deployment, operation and support on security of network and infrastructure in Smartmatic projects. Provide Security Architecture based on Risk Assessment. Develop Business Continuity and Disaster Recovery Plan. Perform Vulnerability assessment, ethical hacking and penetration testing. Advisor on information security issues.



Bancaribe

9 years 11 months

Security Specialist

Aug 2003 - Aug 2008 · 5 years 1 month

Caracas, Venezuela

Planification and Management of Information Security System. Vulnerability and Risk Management. Leader of risk assessment and security evaluation team on Software Development Life Cicle projects. Advisor on information security issues and methodologies. Support on Incident Response Team.

Information Security Administrator

May 2001 - Aug 2003 · 2 years 4 months

Caracas, Venezuela

- 6. As seen from Jesus' LinkedIn profile, he was employed by Smartmatic as their Master Information Security Specialist from August 2008 - March 2017, within the time frame of the registered SSL certificate for Smartmatic and within Venezuela.
- 7. This evidence shows that Smartmatic was indeed connected to Venezuela as well as shows that their dealings with the Philippine's is still on-going as their website is in their election commission servers with matching and current SSL certificates.

I declare under penalty of perjury that the forgoing i this December 16th, 2020.



1.	, hereby state the following:
2.	I am an adult of sound mine. All statements in this declaration are based on my personal knowledge and are true and correct.
3.	I am making this statement voluntarily and on my own initiative. I have not been promised, nor do I expect to receive, anything in exchange for my testimony and giving this statement. I have no expectation of any profit or reward and understand that there are those who may seek to harm me for what I say in this statement. I have not participated in any political process in the United States, have not supported any candidate for office in the United States, am not legally permitted to vote in the United States, and have never attempted to vote in the United States.
4.	I want to alert the public and let the world know the truth about the corruption, manipulation, and lies being committed by a conspiracy of people and companies intent upon betraying the honest people of the United States and their legally constituted institutions and fundamental rights as citizens. This conspiracy began more than a decade ago in Venezuela and has spread to countries all over the world. It is a conspiracy to wrongfully gain and keep power and wealth. It involves political leaders, powerful companies, and other persons whose purpose is to gain and keep power by changing the free will of the people and subverting the
	proper course of governing.
5.	Over the course of my career, I specialized in the marines
6.	Due to my training in special operations and my extensive military and academic formations, I was selected for the national security guard detail of the President of Venezuela.

- Page 1 of 8

7.

8.

		+ 3		
		1 - 400		
16-04				
-	Land of the land	1		
instrumental in taken over the imprisoned. Wi Hugo Chavez President. On President of the and became the Chávez. Cabelle early 2012 and	his gaining power duties of the thin hours of States was released December 11, and United Social esecond most was re-elected Cabello was need president of	ver. In 2002, Some presidency Señor Cabello from prison 2011, Cabello ist Party – the powerful figured president of that post in line for the National	eñor Cabello while Hug taking over and regaine was installe e party of Pr ire in the pa f the Nation n January 20 he presidency ll Assembly	the presidency, d the office of ed as the Vice-resident Chávez arty after Hugo al Assembly in 013. After Hugo y of the country, and yielded to
	NO.			
No. of Concession, Name of Street, or other parts of the Concession, Name of Street, or other parts of the Concession, Name of Street, or other parts of the Concession, Name of Street, or other parts of the Concession, Name of Street, or other parts of the Concession, Name of Street, or other parts of the Concession, Name of Street, or other parts of the Concession, Name of Street, or other parts of the Concession, Name of Street, or other parts of the Concession, Name of Street, or other parts of the Concession, Name of Street, or other parts of the Concession, Name of Street, or other parts of the Concession, Name of Street, or other parts of the Concession, Name of Street, or other parts of the Concession, Name of Street, or other parts of the Concession, Name of Street, or other parts of the Concession, Name of Street, or other parts of the Concession, Name of Street, or other parts of the Concession, Name of Street, or other parts of the Concession, Name of Street, or other parts of the Concession, Name of Street, or other parts of the Concession, Name of Street, or other parts of the Concession, Name of Street, or other parts of the Concession, Name of Street, or other parts of the Concession, Name of Street, or other parts of the Concession, Name of Street, or other parts of the Concession, Name of Street, or other parts of the Concession, Name of Street, or other parts of the Concession, Name of Street, or other parts of the Concession, Name of Street, or other parts of the Concession, Name of Street, or other parts of the Concession, Name of Street, or other parts of the Concession, Name of Street, or other parts of the Concession, Name of Street, or other parts of the Concession, Name of Street, or other parts of the Concession, Name of Street, or other parts of the Concession, Name of Street, or other parts of the Concession, Name of Street, or other parts of the Concession, Name of Street, or other parts of the Concession, Name of Street, or other parts of the Concession, Name of Street, or other pa				
precise and exac			ne details abo	
wanted, where t be done.	ne meeting wa	s to occur, who	was to atte	nd, what was to
		.,		
TOTAL SECTION				
	I was with	ness to the c	reation and	operation of a

- Page 2 of 8

sophisticated electronic voting system that permitted the leaders of the Venezuelan government to manipulate the tabulation of votes for national and local elections and select the winner of those elections in order to gain and maintain their power.

- 11. In mid-February of 2009, there was a national referendum to change the Constitution of Venezuela to end term limits for elected officials, including the President of Venezuela. The referendum passed. This permitted Hugo Chavez to be re-elected an unlimited number of times.
- 12. After passage of the referendum, President Chavez instructed me to make arrangements for him to meet with Jorge Rodriguez, then President of the National Electoral Council, and three executives from Smartmatic. Among the three Smartmatic representatives were
 - President Chavez had multiple meetings with Rodriguez and the Smartmatic team at which I was present. In the first of four meetings, Jorge Rodriguez promoted the idea to create software that would manipulate elections. Chavez was very excited and made it clear that he would provide whatever Smartmatic needed. He wanted them immediately to create a voting system which would ensure that any time anything was going to be voted on the voting system would guarantee results that Chavez wanted. Chavez offered Smartmatic many inducements, including large sums of money, for Smartmatic to create or modify the voting system so that it would guarantee Chavez would win every election cycle. Smartmatic's team agreed to create such a system and did so.
- 13. I arranged and attended three more meetings between President Chavez and the representatives from Smartmatic at which details of the new

- Page 3 of 8

voting system were discussed and agreed upon. For each of these meetings, I communicated directly with on details of where and when to meet, where the participants would be picked up and delivered to the meetings, and what was to be accomplished. At these meetings, the participants called their project the "Chavez revolution." From that point on, Chavez never lost any election. In fact, he was able to ensure wins for himself, his party, Congress persons and mayors from townships.

- 14. Smartmatic's electoral technology was called "Sistema de Gestión Electoral" (the "Electoral Management System"). Smartmatic was a pioneer in this area of computing systems. Their system provided for transmission of voting data over the internet to a computerized central tabulating center. The voting machines themselves had a digital display, fingerprint recognition feature to identify the voter, and printed out the voter's ballot. The voter's thumbprint was linked to a computerized record of that voter's identity. Smartmatic created and operated the entire system.
- 15. Chavez was most insistent that Smartmatic design the system in a way that the system could change the vote of each voter without being detected. He wanted the software itself to function in such a manner that if the voter were to place their thumb print or fingerprint on a scanner, then the thumbprint would be tied to a record of the voter's name and identity as having voted, but that voter would not tracked to the changed vote. He made it clear that the system would have to be setup to not leave any evidence of the changed vote for a specific voter and that there would be no evidence to show and nothing to contradict that the name or the fingerprint or thumb print was going with a changed vote. Smartmatic agreed to create such a system and produced the software and hardware that accomplished that result for President Chavez.
- 16. After the Smartmatic Electoral Management System was put in place, I closely observed several elections where the results were manipulated using Smartmatic software. One such election was in December 2006 when Chavez was running against Rosales. Chavez won with a landslide over Manuel Rosales a margin of nearly 6 million votes for Chavez versus 3.7 million for Rosales.
- 17. On April 14, 2013, I witnessed another Venezuelan national election in which the Smartmatic Electoral Management System was used to manipulate and change the results for the person to succeed Hugo Chávez

- Page 4 of 8

as President. In that election, Nicolás Maduro ran against Capriles Radonsky.

Inside that location was a control room in which there were multiple digital display screens – TV screens – for results of voting in each state in Venezuela. The actual voting results were fed into that room and onto the displays over an internet feed, which was connected to a sophisticated computer system created by Smartmatic. People in that room were able to see in "real time" whether the vote that came through the electronic voting system was in their favor or against them. If one looked at any particular screen, they could determine that the vote from any specific area or as a national total was going against either candidate. Persons controlling the vote tabulation computer had the ability to change the reporting of votes by moving votes from one candidate to another by using the Smartmatic software.

- 18. By two o'clock in the afternoon on that election day Capriles Radonsky was ahead of Nicolás Maduro by two million votes. When Maduro and his supporters realized the size of Radonsky's lead they were worried that they were in a crisis mode and would lose the election. The Smartmatic machines used for voting in each state were connected to the internet and reported their information over the internet to the Caracas control center in real-time. So, the decision was made to reset the entire system. Maduro's and his supporters ordered the network controllers to take the internet itself offline in practically all parts in Venezuela and to change the results.
- 19. It took the voting system operators approximately two hours to make the adjustments in the vote from Radonsky to Maduro. Then, when they turned the internet back on and the on-line reporting was up and running again, they checked each screen state by state to be certain where they could see that each vote was changed in favor of Nicholas Maduro. At that moment the Smartmatic system changed votes that were for Capriles Radonsky to Maduro. By the time the system operators finish, they had achieved a convincing, but narrow victory of 200,000 votes for Maduro.
- 20. After Smartmatic created the voting system President Chavez wanted, he exported the software and system all over Latin America. It was sent to Bolivia, Nicaragua, Argentina, Ecuador, and Chile countries that were in alliance with President Chavez. This was a group of leaders who wanted to be able to guarantee they maintained power in their countries. When Chavez died, Smartmatic was in a position of being the only

- Page 5 of 8

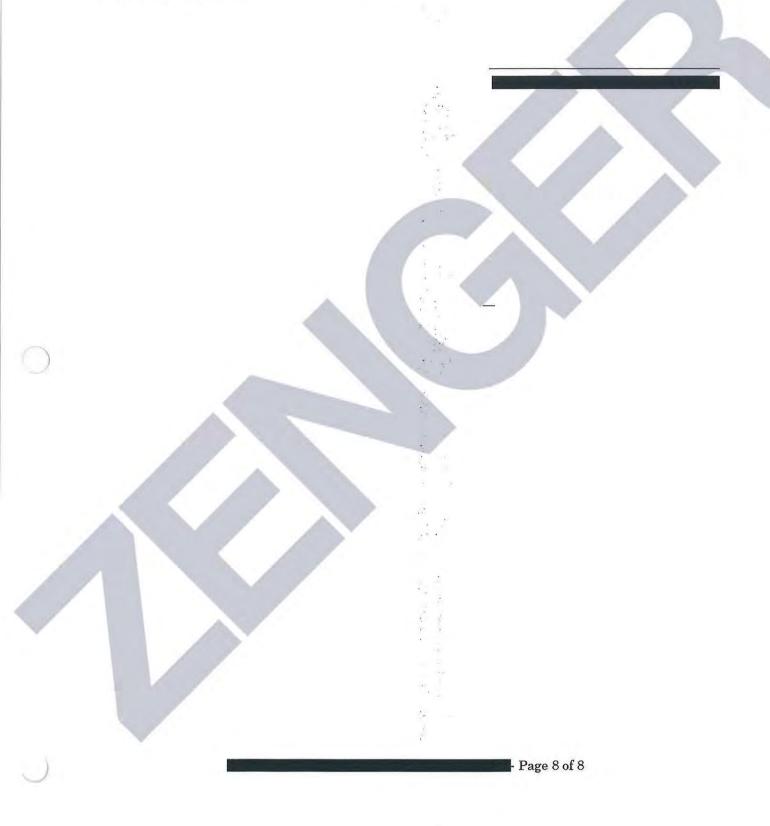
company that could guarantee results in Venezuelan elections for the party in power.

- 21. I want to point out that the software and fundamental design of the electronic electoral system and software of Dominion and other election tabulating companies relies upon software that is a descendant of the Smartmatic Electoral Management System. In short, the Smartmatic software is in the DNA of every vote tabulating company's software and system.
- 22. Dominion is one of three major companies that tabulates votes in the United States. Dominion uses the same methods and fundamentally same software design for the storage, transfer and computation of voter identification data and voting data. Dominion and Smartmatic did business together. The software, hardware and system have the same fundamental flaws which allow multiple opportunities to corrupt the data and mask the process in a way that the average person cannot detect any fraud or manipulation. The fact that the voting machine displays a voting result that the voter intends and then prints out a paper ballot which reflects that change does not matter. It is the software that counts the digitized vote and reports the results. The software itself is the one that changes the information electronically to the result that the operator of the software and vote counting system intends to produce that counts. That's how it is done. So the software, the software itself configures the vote and voting result -- changing the selection made by the voter. The software decides the result regardless of what the voter votes.
- 23. All of the computer controlled voting tabulation is done in a closed environment so that the voter and any observer cannot detect what is taking place unless there is a malfunction or other event which causes the observer to question the process. I saw first-hand that the manipulation and changing of votes can be done in real-time at the secret counting center which existed in Caracas, Venezuela. For me it was something very surprising and disturbing. I was in awe because I had never been present to actually see it occur and I saw it happen. So, I learned first-hand that it doesn't matter what the voter decides or what the paper ballot says. It's the software operator and the software that decides what counts not the voter.

24.	If one questions the reliability of the words of	of my observations, they only have to read
7		a time period in
		- Page 6 of 8

	which Smartmatic had possession of all the votes and the voting, the votes themselves and the voting information at their disposition in Venezuela.
	he was assuring that the voting system implemented or used by Smartmatic was completely secure, that it could not be compromised, was not able to be altered.
25.	But later, in 2017 when there were elections where Maduro was running and elections for legislators in Venezuela, and Smartmatic broke their secrecy pact with the government of Venezuela. He made a public announcement through the media in which he stated that all the Smartmatic voting machines used during those elections were totally manipulated and they were manipulated by the electoral council of Venezuela back then. stated that all of the votes for Nicholas Maduro and the other persons running for the legislature were manipulated and they actually had lost. So I think that's the greatest proof that the fraud can be carried out and will be denied by the software company that admitted publicly that Smartmatic had created, used and still uses vote counting software that can be manipulated or altered.
26.	I am alarmed because of what is occurring in plain sight during this 2020 election for President of the United States. The circumstances and events are eerily reminiscent of what happened with Smartmatic software electronically changing votes in the 2013 presidential election in Venezuela. What happened in the United States was that the vote counting was abruptly stopped in five states using Dominion software. At the time that vote counting was stopped, Donald Trump was significantly ahead in the votes. Then during the wee hours of the morning, when there was no voting occurring and the vote count reporting was off-line, something significantly changed. When the vote reporting resumed the very next morning there was a very pronounced change in voting in favor of the opposing candidate, Joe Biden.
27.	I have worked in gathering information, researching, and working with information technology. That's what I know how to do and the special knowledge that I have. Due to these recent election events, I contacted a number of reliable and intelligent ex-co-workers of mine that are still informants and work with the intelligence community. I asked for them to give me information that was up-to-date information in as far as how all these businesses are acting, what actions they are taking.
	- Page 7 of 8

I declare under penalty of perjury that the foregoing is true and correct and that this Declaration was prepared in Dallas County, State of Texas, and executed on November 15, 2020.



Executive Orders

Executive Order on Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election

Issued on: September 12, 2018

By the authority vested in me as President by the Constitution and the laws of the United States of America, including the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) (IEEPA), the National Emergencies Act (50 U.S.C. 1601 et seq.) (NEA), section 212(f) of the Immigration and Nationality Act of 1952 (8 U.S.C. 1182(f)), and section 301 of title 3, United States Code,

I, DONALD J. TRUMP, President of the United States of America, find that the ability of persons located, in whole or in substantial part, outside the United States to interfere in or undermine public confidence in United States elections, including through the unauthorized accessing of election and campaign infrastructure or the covert distribution of propaganda and disinformation, constitutes an unusual and extraordinary threat to the national security and foreign policy of the United States. Although there has been no evidence of a foreign power altering the outcome or vote tabulation in any United States election, foreign powers have historically sought to exploit America's free and open political system. In recent years, the proliferation of digital devices and internet-based communications has created significant vulnerabilities and magnified the scope and intensity of the threat of foreign interference, as illustrated in the 2017 Intelligence Community Assessment. I hereby declare a national emergency to deal with this threat.

Accordingly, I hereby order:

Section 1. (a) Not later than 45 days after the conclusion of a United States election, the Director of National Intelligence, in consultation with the heads of any other appropriate executive departments and agencies (agencies), shall conduct an assessment of any information indicating that a foreign government, or any person acting as an agent of or on behalf of a foreign government, has acted with the intent or purpose of interfering in that election. The assessment shall identify, to the maximum extent ascertainable, the nature of any foreign interference and any methods employed to execute it, the persons involved, and the foreign government or governments that authorized, directed, sponsored, or supported it. The Director of National Intelligence shall deliver this assessment and appropriate supporting information to the President, the Secretary of State, the Secretary of the Treasury, the Secretary of Defense, the Attorney General, and the Secretary of Homeland Security.

- (b) Within 45 days of receiving the assessment and information described in section 1(a) of this order, the Attorney General and the Secretary of Homeland Security, in consultation with the heads of any other appropriate agencies and, as appropriate, State and local officials, shall deliver to the President, the Secretary of State, the Secretary of the Treasury, and the Secretary of Defense a report evaluating, with respect to the United States election that is the subject of the assessment described in section 1(a):
- (i) the extent to which any foreign interference that targeted election infrastructure materially affected the security or integrity of that infrastructure, the tabulation of votes, or the timely transmission of election results; and
- (ii) if any foreign interference involved activities targeting the infrastructure of, or pertaining to, a political organization, campaign, or candidate, the extent to which such activities materially affected the security or integrity of that infrastructure, including by unauthorized access to, disclosure or threatened disclosure of, or alteration or falsification of, information or data.

The report shall identify any material issues of fact with respect to these matters that the Attorney General and the Secretary of Homeland Security are unable to evaluate or reach agreement on at the time the report is submitted. The report shall also include updates and recommendations, when appropriate, regarding remedial actions to be taken by the United States Government, other than the sanctions described in sections 2 and 3 of this order.

- (c) Heads of all relevant agencies shall transmit to the Director of National Intelligence any information relevant to the execution of the Director's duties pursuant to this order, as appropriate and consistent with applicable law. If relevant information emerges after the submission of the report mandated by section 1(a) of this order, the Director, in consultation with the heads of any other appropriate agencies, shall amend the report, as appropriate, and the Attorney General and the Secretary of Homeland Security shall amend the report required by section 1(b), as appropriate.
- (d) Nothing in this order shall prevent the head of any agency or any other appropriate official from tendering to the President, at any time through an appropriate channel, any analysis, information, assessment, or evaluation of foreign interference in a United States election.
- (e) If information indicating that foreign interference in a State, tribal, or local election within the United States has occurred is identified, it may be included, as appropriate, in the assessment mandated by section 1(a) of this order or in the report mandated by section 1(b) of this order, or submitted to the President in an independent report.
- (f) Not later than 30 days following the date of this order, the Secretary of State, the Secretary of the Treasury, the Attorney General, the Secretary of Homeland Security, and the Director of National Intelligence shall develop a framework for the process that will be used to carry out their respective responsibilities pursuant to this order. The framework, which may be classified in whole or in part, shall focus on ensuring that agencies fulfill their responsibilities pursuant to this order in a manner that maintains methodological consistency; protects law enforcement or other sensitive information and intelligence sources and methods; maintains an appropriate

separation between intelligence functions and policy and legal judgments; ensures that efforts to protect electoral processes and institutions are insulated from political bias; and respects the principles of free speech and open debate.

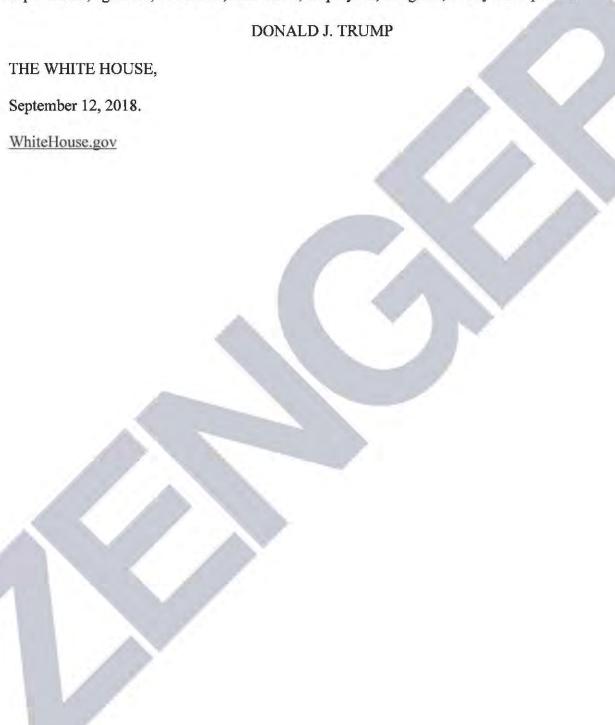
- Sec. 2. (a) All property and interests in property that are in the United States, that hereafter come within the United States, or that are or hereafter come within the possession or control of any United States person of the following persons are blocked and may not be transferred, paid, exported, withdrawn, or otherwise dealt in: any foreign person determined by the Secretary of the Treasury, in consultation with the Secretary of State, the Attorney General, and the Secretary of Homeland Security:
- (i) to have directly or indirectly engaged in, sponsored, concealed, or otherwise been complicit in foreign interference in a United States election;
- (ii) to have materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, any activity described in subsection (a)(i) of this section or any person whose property and interests in property are blocked pursuant to this order; or
- (iii) to be owned or controlled by, or to have acted or purported to act for or on behalf of, directly or indirectly, any person whose property or interests in property are blocked pursuant to this order.
- (b) Executive Order 13694 of April 1, 2015, as amended by Executive Order 13757 of December 28, 2016, remains in effect. This order is not intended to, and does not, serve to limit the Secretary of the Treasury's discretion to exercise the authorities provided in Executive Order 13694. Where appropriate, the Secretary of the Treasury, in consultation with the Attorney General and the Secretary of State, may exercise the authorities described in Executive Order 13694 or other authorities in conjunction with the Secretary of the Treasury's exercise of authorities provided in this order.
- (c) The prohibitions in subsection (a) of this section apply except to the extent provided by statutes, or in regulations, orders, directives, or licenses that may be issued pursuant to this order, and notwithstanding any contract entered into or any license or permit granted prior to the date of this order.
- Sec. 3. Following the transmission of the assessment mandated by section 1(a) and the report mandated by section 1(b):
- (a) the Secretary of the Treasury shall review the assessment mandated by section 1(a) and the report mandated by section 1(b), and, in consultation with the Secretary of State, the Attorney General, and the Secretary of Homeland Security, impose all appropriate sanctions pursuant to section 2(a) of this order and any appropriate sanctions described in section 2(b) of this order; and

- (b) the Secretary of State and the Secretary of the Treasury, in consultation with the heads of other appropriate agencies, shall jointly prepare a recommendation for the President as to whether additional sanctions against foreign persons may be appropriate in response to the identified foreign interference and in light of the evaluation in the report mandated by section 1(b) of this order, including, as appropriate and consistent with applicable law, proposed sanctions with respect to the largest business entities licensed or domiciled in a country whose government authorized, directed, sponsored, or supported election interference, including at least one entity from each of the following sectors: financial services, defense, energy, technology, and transportation (or, if inapplicable to that country's largest business entities, sectors of comparable strategic significance to that foreign government). The recommendation shall include an assessment of the effect of the recommended sanctions on the economic and national security interests of the United States and its allies. Any recommended sanctions shall be appropriately calibrated to the scope of the foreign interference identified, and may include one or more of the following with respect to each targeted foreign person:
- (i) blocking and prohibiting all transactions in a person's property and interests in property subject to United States jurisdiction;
- (ii) export license restrictions under any statute or regulation that requires the prior review and approval of the United States Government as a condition for the export or re-export of goods or services;
- (iii) prohibitions on United States financial institutions making loans or providing credit to a person;
- (iv) restrictions on transactions in foreign exchange in which a person has any interest;
- (v) prohibitions on transfers of credit or payments between financial institutions, or by, through, or to any financial institution, for the benefit of a person;
- (vi) prohibitions on United States persons investing in or purchasing equity or debt of a person;
- (vii) exclusion of a person's alien corporate officers from the United States;
- (viii) imposition on a person's alien principal executive officers of any of the sanctions described in this section; or
- (ix) any other measures authorized by law.
- Sec. 4. I hereby determine that the making of donations of the type of articles specified in section 203(b)(2) of IEEPA (50 U.S.C. 1702(b)(2)) by, to, or for the benefit of any person whose property and interests in property are blocked pursuant to this order would seriously impair my ability to deal with the national emergency declared in this order, and I hereby prohibit such donations as provided by section 2 of this order.
- Sec. 5. The prohibitions in section 2 of this order include the following:

- (a) the making of any contribution or provision of funds, goods, or services by, to, or for the benefit of any person whose property and interests in property are blocked pursuant to this order; and
- (b) the receipt of any contribution or provision of funds, goods, or services from any such person.
- Sec. 6. I hereby find that the unrestricted immigrant and nonimmigrant entry into the United States of aliens whose property and interests in property are blocked pursuant to this order would be detrimental to the interests of the United States, and I hereby suspend entry into the United States, as immigrants or nonimmigrants, of such persons. Such persons shall be treated as persons covered by section 1 of Proclamation 8693 of July 24, 2011 (Suspension of Entry of Aliens Subject to United Nations Security Council Travel Bans and International Emergency Economic Powers Act Sanctions).
- Sec. 7. (a) Any transaction that evades or avoids, has the purpose of evading or avoiding, causes a violation of, or attempts to violate any of the prohibitions set forth in this order is prohibited.
- (b) Any conspiracy formed to violate any of the prohibitions set forth in this order is prohibited.
- Sec. 8. For the purposes of this order:
- (a) the term "person" means an individual or entity;
- (b) the term "entity" means a partnership, association, trust, joint venture, corporation, group, subgroup, or other organization;
- (c) the term "United States person" means any United States citizen, permanent resident alien, entity organized under the laws of the United States or any jurisdiction within the United States (including foreign branches), or any person (including a foreign person) in the United States;
- (d) the term "election infrastructure" means information and communications technology and systems used by or on behalf of the Federal Government or a State or local government in managing the election process, including voter registration databases, voting machines, voting tabulation equipment, and equipment for the secure transmission of election results;
- (e) the term "United States election" means any election for Federal office held on, or after, the date of this order;
- (f) the term "foreign interference," with respect to an election, includes any covert, fraudulent, deceptive, or unlawful actions or attempted actions of a foreign government, or of any person acting as an agent of or on behalf of a foreign government, undertaken with the purpose or effect of influencing, undermining confidence in, or altering the result or reported result of, the election, or undermining public confidence in election processes or institutions;

- (g) the term "foreign government" means any national, state, provincial, or other governing authority, any political party, or any official of any governing authority or political party, in each case of a country other than the United States;
- (h) the term "covert," with respect to an action or attempted action, means characterized by an intent or apparent intent that the role of a foreign government will not be apparent or acknowledged publicly; and
- (i) the term "State" means the several States or any of the territories, dependencies, or possessions of the United States.
- Sec. 9. For those persons whose property and interests in property are blocked pursuant to this order who might have a constitutional presence in the United States, I find that because of the ability to transfer funds or other assets instantaneously, prior notice to such persons of measures to be taken pursuant to this order would render those measures ineffectual. I therefore determine that for these measures to be effective in addressing the national emergency declared in this order, there need be no prior notice of a listing or determination made pursuant to section 2 of this order.
- Sec. 10. Nothing in this order shall prohibit transactions for the conduct of the official business of the United States Government by employees, grantees, or contractors thereof.
- Sec. 11. The Secretary of the Treasury, in consultation with the Attorney General and the Secretary of State, is hereby authorized to take such actions, including the promulgation of rules and regulations, and to employ all powers granted to the President by IEEPA as may be necessary to carry out the purposes of this order. The Secretary of the Treasury may re-delegate any of these functions to other officers within the Department of the Treasury consistent with applicable law. All agencies of the United States Government are hereby directed to take all appropriate measures within their authority to carry out the provisions of this order.
- Sec. 12. The Secretary of the Treasury, in consultation with the Attorney General and the Secretary of State, is hereby authorized to submit the recurring and final reports to the Congress on the national emergency declared in this order, consistent with section 401(c) of the NEA (50 U.S.C. 1641(c)) and section 204(c) of IEEPA (50 U.S.C. 1703(c)).
- Sec. 13. This order shall be implemented consistent with 50 U.S.C. 1702(b)(1) and (3).
- Sec. 14. (a) Nothing in this order shall be construed to impair or otherwise affect:
- (i) the authority granted by law to an executive department or agency, or the head thereof; or
- (ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.
- (b) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(c) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.



50 U.S. Code § 1702 - Presidential authorities

- (a) In general
- (1) At the times and to the extent specified in <u>section 1701 of this title</u>, the President may, under such regulations as he may prescribe, by means of instructions, licenses, or otherwise— (A) investigate, regulate, or prohibit—
- (i)

any transactions in foreign exchange,

(ii)

transfers of credit or payments between, by, through, or to any banking institution, to the extent that such transfers or payments involve any interest of any foreign country or a national thereof, (iii)

the importing or exporting of currency or securities,

by any person, or with respect to any property, subject to the jurisdiction of the United States;

investigate, block during the pendency of an investigation, regulate, direct and compel, nullify, void, prevent or prohibit, any acquisition, holding, withholding, use, transfer, withdrawal, transportation, importation or exportation of, or dealing in, or exercising any right, power, or privilege with respect to, or transactions involving, any property in which any foreign country or a national thereof has any interest by any person, or with respect to any property, subject to the jurisdiction of the United States; and.[1]

(C) when the United States is engaged in armed hostilities or has been attacked by a foreign country or foreign nationals, confiscate any property, subject to the jurisdiction of the United States, of any foreign person, foreign organization, or foreign country that he determines has planned, authorized, aided, or engaged in such hostilities or attacks against the United States; and all right, title, and interest in any property so confiscated shall vest, when, as, and upon the terms directed by the President, in such agency or person as the President may designate from time to time, and upon such terms and conditions as the President may prescribe, such interest or property shall be held, used, administered, liquidated, sold, or otherwise dealt with in the interest of and for the benefit of the United States, and such designated agency or person may perform any and all acts incident to the accomplishment or furtherance of these purposes.

(2)

In exercising the authorities granted by paragraph (1), the President may require any person to keep a full record of, and to furnish under oath, in the form of reports or otherwise, complete information relative to any act or transaction referred to in paragraph (1) either before, during, or after the completion thereof, or relative to any interest in foreign property, or relative to any property in which any foreign country or any national thereof has or has had any interest, or as may be otherwise necessary to enforce the provisions of such paragraph. In any case in which a report by a person could be required under this paragraph, the President may require the production of any books of account, records, contracts, letters, memoranda, or other papers, in the custody or control of such person.

(3)

Compliance with any regulation, instruction, or direction issued under this chapter shall to the extent thereof be a full acquittance and discharge for all purposes of the obligation of the person making the same. No person shall be held liable in any court for or with respect to anything done or omitted in good faith in connection with the administration of, or pursuant to and in reliance on, this chapter, or any regulation, instruction, or direction issued under this chapter.

- (b) Exceptions to grant of authority The authority granted to the President by this section does not include the authority to regulate or prohibit, directly or indirectly—
- any postal, telegraphic, telephonic, or other personal communication, which does not involve a transfer of anything of value;
- donations, by persons subject to the jurisdiction of the United States, of articles, such as food, clothing, and medicine, intended to be used to relieve human suffering, except to the extent that the President determines that such donations (A) would seriously impair his ability to deal with any national emergency declared under section 1701 of this title, (B) are in response to coercion against the proposed recipient or donor, or (C) would endanger Armed Forces of the United States which are engaged in hostilities or are in a situation where imminent involvement in hostilities is clearly indicated by the circumstances; or [2]
- the importation from any country, or the exportation to any country, whether commercial or otherwise, regardless of format or medium of transmission, of any information or informational materials, including but not limited to, publications, films, posters, phonograph records, photographs, microfilms, microfiche, tapes, compact disks, CD ROMs, artworks, and news wire feeds. The exports exempted from regulation or prohibition by this paragraph do not include those which are otherwise controlled for export under section 4604 [3] of this title, or under section 4605 [3] of this title to the extent that such controls promote the nonproliferation or antiterrorism policies of the United States, or with respect to which acts are prohibited by chapter 37 of title 18; or
- (4) any transactions ordinarily incident to travel to or from any country, including importation of accompanied baggage for personal use, maintenance within any country including payment of living expenses and acquisition of goods or services for personal use, and arrangement or facilitation of such travel including nonscheduled air, sea, or land voyages. (c) Classified information

In any judicial review of a determination made under this section, if the determination was based on classified information (as defined in section 1(a) of the <u>Classified Information Procedures</u>

<u>Act</u>) such information may be submitted to the reviewing court ex parte and in camera. This subsection does not confer or imply any right to judicial review.

(Pub. L. 95–223, title II, § 203, Dec. 28, 1977, 91 Stat. 1626; Pub. L. 100–418, title II, § 2502(b)(1), Aug. 23, 1988, 102 Stat. 1371; Pub. L. 103–236, title V, § 525(c)(1), Apr. 30, 1994, 108 Stat. 474; Pub. L. 107–56, title I, § 106, Oct. 26, 2001, 115 Stat. 277.)

Congress of the United States

Washington, DC 20515

October 6, 2006

Henry M. Paulson, Jr. Secretary Department of the Treasury 1500 Pennsylvania Ave., N.W. Washington, D.C. 20220

Dear Mr. Secretary:

I am writing to follow up on my letter of May 4, 2006, to Secretary Snow, seeking review by the Committee on Foreign Investment in the United States of the acquisition of Sequoia Voting Systems by Smartmatic, a foreign-owned company. I believe this transaction raises exactly the sort of foreign ownership issues that CFIUS is best positioned to examine for national security concerns. As discussed below, publicly reported information about Smartmatic's ownership and about the vulnerability of electronic voting machines to tampering raises serious concerns. I strongly urge CFIUS to independently verify the information provided to American officials and the public by Sequoia/Smartmatic, and to take all appropriate measures to safeguard our national security.

It is undisputed that Smartmatic is foreign-owned and it has acquired Sequoia, one of the three major voting machine companies doing business in the U.S. According to a Sequoia press release in May 2006 (copy attached) Sequoia voting machines were used to record over 125 million votes during the 2004 Presidential election in the United States. As we confront another election, Americans deserve to know that the Administration has made sure that any foreign ownership of voting machines poses no national security threat.

Although many press reports have tried, it appears that it is not possible to discern the true owners of Smartmatic from information available to the public. Smartmatic now acknowledges that Antonio Mugica, a Venezuelan businessman, has a controlling interest in Smartmatic, but the company has not revealed who all the other Smartmatic owners are. According to the press, Smartmatic's owners are hidden through a web of off-shore private entities. (See attached articles.)

The opaque nature of Smartmatic's ownership is particularly troubling since Smartmatic has been associated by the press with the Venezuelan government led by Hugo Chavez, which is openly hostile to the United States. According to press reports, Smartmatic shared a founder, officers, directors and a principal place of business with Bizta, a company in which, according to Smartmatic, the Venezuelan government previously held a 28% stake. Mugica is also a director of Bizta.

Henry M. Paulson, Jr. October 6, 2006 Page 2

According to Smartmatic press releases, (copies attached) Smartmatic and Bizta were part of the consortium that received the government contract to provide the voting machines for the 2004 referendum election to recall Chavez as Venezuela's president, and have since been awarded other contracts by the Venezuelan government.

Smartmatic's possible connection to the Venezuelan government poses a potential national security concern in the context of its acquisition of Sequoia because electronic voting machines are susceptible to tampering and insiders are in the best position to engage in such tampering. The 2005 Government Accountability Office Report on electronic voting, GAO-05-956, and other private sector studies consistently support this conclusion. Thus, the reports that Sequoia brought Venezuelan nationals to the United States to work on the Chicago 2006 primary election raises questions about whether these individuals are subject to direction from a foreign interest that might pose a threat to the integrity of the election. Similarly, the use of Smartmatic software and machines developed in Venezuela, such as the HAAT software that was at issue in Chicago, raises questions as to whether this software is susceptible to manipulation by its unknown creators. Reportedly, Smartmatic may soon be introducing into the United States the type of electronic voting machines that were used (with Bizta software) in the controversial 2004 Venezuelan recall election, under the label AVC Edge II Plus.

In reviewing the Smartmatic acquisition of Sequoia, it is important that CFIUS understand the products and services that are of Venezuelan origin and evaluate Smartmatic's ownership to determine who could have influence and control over these and other Sequoia products and services that are in use or intended for use in U.S. elections. In light of Smartmatic's failure fully to answer these questions to date, this issue demands the most thorough independent investigation by CFIUS.

Thank you for your consideration of this letter.

Sincerely,

Member of Congress

Attachments

Congress of the United States

Washington, DC 20510

December 6, 2019

Michael McCarthy Chairman McCarthy Group, LLC

Dear Mr. McCarthy:

We are writing to request information regarding McCarthy Group, LLC's (McCarthy Group) investment in Election Systems & Software (ES&S), one of three election technology vendors responsible for developing, manufacturing and maintaining the vast majority of voting machines and software in the United States, and to request information about your firm's structure and finances as it relates to this company.

Some private equity funds operate under a model where they purchase controlling interests in companies and implement drastic cost-cutting measures at the expense of consumers, workers, communities, and taxpayers. Recent examples include Toys "R" Us and Shopko.¹ For that reason, we have concerns about the spread and effect of private equity investment in many sectors of the economy, including the election technology industry—an integral part of our nation's democratic process. We are particularly concerned that secretive and "trouble-plagued companies,"² owned by private equity firms and responsible for manufacturing and maintaining voting machines and other election administration equipment, "have long skimped on security in favor of convenience," leaving voting systems across the country "prone to security problems."³ In light of these concerns, we request that you provide information about your firm, the portfolio companies in which it has invested, the performance of those investments, and the ownership and financial structure of your funds.

Over the last two decades, the election technology industry has become highly concentrated, with a handful of consolidated vendors controlling the vast majority of the market. In the early

¹ Atlantic, "The Demise of Toys 'R' Us Is a Warning," Bryce Covert, July/August 2018 issue, https://www.theatlantic.com/magazine/archive/2018/07/toys-r-us-bankruptcy-private-equity/561758/; Axios, "How workers suffered from Shopko's bankruptcy while Sun Capital made money," Dan Primack, "How workers suffered from Shopko's bankruptcy while Sun Capital made money," June 11, 2019, https://www.axios.com/shopko-bankruptcy-sun-capital-547b97ba-901c-4201-92cc-6d3168357fa3.html.

² ProPublica, "The Market for Voting Machines Is Broken. This Company Has Thrived in It.," Jessica Huseman, October 28, 2019, https://www.propublica.org/article/the-market-for-voting-machines-is-broken-this-company-has-thrived-in-it.

Associated Press News, "US Election Integrity Depends on Security-Challenged Firms," Frank Bajak, October 28, 2019, https://apnews.com/f6876669cb6b4e4c9850844f8e015b4c.

2000s, almost twenty vendors competed in the election technology market.⁴ Today, three large vendors—ES&S, Dominion Voting Systems, and Hart InterCivic—collectively provide voting machines and software that facilitate voting for over 90% of all eligible voters in the United States.⁵ Private equity firms reportedly own or control each of these vendors, with very limited "information available in the public domain about their operations and financial performance." While experts estimate that the total revenue for election technology vendors is about \$300 million, there is no publicly available information on how much those vendors dedicate to research and development, maintenance of voting systems, or profits and executive compensation.⁷

Concentration in the election technology market and the fact that vendors are often "more seasoned in voting machine and technical services contract negotiations" than local election officials, give these companies incredible power in their negotiations with local and state governments. As a result, jurisdictions are often caught in expensive agreements in which the same vendor both sells or leases, and repairs and maintains voting systems—leaving local officials dependent on the vendor, and the vendor with little incentive to substantially overhaul and improve its products. In fact, the Election Assistance Commission (EAC), the primary federal body responsible for developing voluntary guidance on voting technology standards, advises state and local officials to consider "the cost to purchase or lease, operate, and maintain a voting system over its life span ... [and to] know how the vendor(s) plan to be profitable" when signing contracts, because vendors typically make their profits by ensuring "that they will be around to maintain it after the sale." The EAC has warned election officials that "[i]f you do not manage the vendors, they will manage you."

Election security experts have noted for years that our nation's election systems and infrastructure are under serious threat. In January 2017, the U.S. Department of Homeland Security designated the United States' election infrastructure as "critical infrastructure" in order to prioritize the protection of our elections and to more effectively assist state and local election officials in addressing these risks. ¹⁰ However, voting machines are reportedly falling apart across the country, as vendors neglect to innovate and improve important voting systems, putting our

⁴ Bloomberg, "Private Equity Controls the Gatekeepers of American Democracy," Anders Melin and Reade Pickert, November 3, 2018, https://www.bloomberg.com/news/articles/2018-11-03/private-equity-controls-the-gatekeepers-of-american-democracy.

⁵ Penn Wharton Public Policy Initiative, "The Business of Voting," July 2018, https://publicpolicy.wharton.upenn.edu/live/files/270-the-business-of-voting.

⁶ Id.

⁷ Id.

⁸ Brennan Center for Justice, "America's Voting Machines at Risk," Lawrence Norden and Christopher Famighetti, 2015, https://www.brennancenter.org/sites/default/files/publications/Americas Voting Machines At Risk.pdf; Penn Wharton Public Policy Initiative, "The Business of Voting," July 2018, https://publicpolicy.wharton.upenn.cdu/live/files/270-the-business-of-voting.

⁹ U.S. Election Assistance Commission, "Ten Things to Know About Selecting a Voting System," October 14, 2017, https://www.eac.gov/documents/2017/10/14/ten-things-to-know-about-selecting-a-voting-system-cybersecurity-voting-systems-voting-technology/.

Department of Homeland Security, "Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector," January 6, 2017, https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical.

elections at avoidable and increased risk, 11 In 2015, election officials in at least 31 states. representing approximately 40 million registered voters, reported that their voting machines needed to be updated, with almost every state "using some machines that are no longer manufactured."12 Moreover, even when state and local officials work on replacing antiquated machines, many continue to "run on old software that will soon be outdated and more vulnerable to hackers."13

In 2018 alone "voters in South Carolina [were] reporting machines that switched their votes after they'd inputted them, scanners [were] rejecting paper ballots in Missouri, and busted machines [were] causing long lines in Indiana."14 In addition, researchers recently uncovered previously undisclosed vulnerabilities in "nearly three dozen backend election systems in 10 states." And, just this year, after the Democratic candidate's electronic tally showed he received an improbable 164 votes out of 55,000 cast in a Pennsylvania state judicial election in 2019, the county's Republican Chairwoman said, "[n]othing went right on Election Day. Everything went wrong. That's a problem."16 These problems threaten the integrity of our elections and demonstrate the importance of election systems that are strong, durable, and not vulnerable to attack.

McCarthy Group reportedly owns or has had investments in ES&S, a major election technology vendor. In order to help us understand your firm's role in this sector, we ask that you provide answers to the following questions no later than December 20, 2019.

- 1. Please provide the disclosure documents and information enumerated in Sections 501 and 503 of the Stop Wall Street Looting Act. 17
- 2. Which election technology companies, including all affiliates or related entities, does McCarthy Group have a stake in or own? Please provide the name of and a brief description of the services each company provides.
 - a. Which election technology companies, including all affiliates or related entities, has McCarthy Group had a stake in or owned in the past twenty

¹¹ AP News, "US election integrity depends on security-challenged firms," Frank Bajak, October 29, 2018, https://apnews.com/f6876669cb6b4e4c9850844f8e015b4c; Penn Wharton Public Policy Initiative, "The Business of Voting," July 2018, https://publicpolicy.wharton.upenn.edu/live/files/270-the-business-of-voting.

¹² Brennan Center for Justice, "America's Voting Machines at Risk," Lawrence Norden and Christopher Famighetti. 2015, https://www.brennancenter.org/sites/default/files/publications/Americas Voting Machines At Risk.pdf. ¹³ Associated Press, "AP Exclusive: New election systems use vulnerable software," Tami Abdollah, July 13, 2019,

https://apnews.com/e5e070c31f3c497fa9e6875f426ccde1.

¹⁴ Vice, "Here's Why All the Voting Machines Are Broken and the Lines Are Extremely Long," Jason Koebler and Matthew Gault, November 6, 2018, https://www.vice.com/en_us/article/59vzgn/heres-why-all-the-voting-machinesare-broken-and-the-lines-are-extremely-long.

¹⁵ Vice, "Exclusive: Critical U.S. Election Systems Have Been Left Exposed Online Despite Official Denials," Kim Zetter, August 8, 2019, https://www.vice.com/en_us/article/3kxzk9/exclusive-critical-us-election-systems-havebeen-left-exposed-online-despite-official-denials.

¹⁶ New York Times, "A Pennsylvania Country's Election Day Nightmare Underscores Voting Machine Concerns," Nick Corasaniti, November 30, 2019, https://www.nytimes.com/2019/11/30/us/politics/pennsylvania-votingmachines.html.

17 Stop Wall Street Looting Act, S.2155, https://www.congress.gov/bill/116th-congress/senate-bill/2155.

- years? Please provide the name of and a brief description of the services each company provides or provided.
- b. For each election technology company McCarthy Group had a stake in or owned in the past twenty years, including all affiliates or related entities, please provide the following information for each year that the firm has had a stake in or owned this company and the five years preceding the firm's investment.
 - i. The name of the company
 - ii. Ownership stake
 - iii. Total revenue
 - iv. Net income
 - v. Percentage of revenue dedicated to research and development
 - vi. Total number of employees
 - vii. A list of all state and local jurisdictions with which the company has a contract to provide election related products or services
 - viii. Other private-equity firms that own a stake in the company
- 3. Has any election technology company, including all affiliates or related entities, in which McCarthy Group has an ownership stake or has had an ownership stake in the last twenty years, been found to have been in noncompliance with the EAC's Voluntary Voting System Guidelines? If so, please provide a copy of each EAC noncompliance notice received by the company and a description of what steps the company took to resolve each issue.
- 4. Has any election technology company, including all affiliates or related entities, in which McCarthy Group has an ownership stake or has had an ownership stake in the last twenty years, been found to have been in noncompliance with any state or local voting system guidelines or practices? If so, please provide a list of all such instances and a description of what steps the company took to resolve each issue.
- 5. Has any election technology company, including all affiliates or related entities, in which McCarthy Group has an ownership stake or has had an ownership stake in the last twenty years, been found to have violated any federal or state laws or regulations? If so, please provide a complete list, including the date and description, of all such violations.
- 6. Has any election technology company, including all affiliates or related entities, in which McCarthy Group has an ownership stake or has had an ownership stake in the last twenty years, reached a settlement with any federal or state law enforcement entity related to a potential violation of any federal or state laws or regulations? If so, please provide a complete list, including the date and description, of all such settlements.
- 7. Has any election technology company, including all affiliates or related entities, in which McCarthy Group has an ownership stake or has had an ownership stake in the

past twenty years, reached a settlement with any state or local jurisdiction related to a potential violation of or breach of contract? If so, please provide a complete list, including the date and description, of all such settlements.

Thank you for your attention to this matter.

Sincerely,

Elizabeth Warren

United States Senator

Amy Klebuchar

United States Senator

Ron Wyden

United States Senator

Mark Pocan

Member of Congress

Congress of the United States

Washington, DC 20510

December 6, 2019

Sami Mnaymneh Founder and Co-Chief Executive Officer H.I.G. Capital, LLC

Tony Tamer
Founder and Co-Chief Executive Officer
H.I.G. Capital, LLC

Dear Messrs. Mnaymneh and Tamer:

We are writing to request information regarding H.I.G. Capital's (H.I.G.) investment in Hart InterCivic Inc. (Hart InterCivic) one of three election technology vendors responsible for developing, manufacturing and maintaining the vast majority of voting machines and software in the United States, and to request information about your firm's structure and finances as it relates to this company.

Some private equity funds operate under a model where they purchase controlling interests in companies and implement drastic cost-cutting measures at the expense of consumers, workers, communities, and taxpayers. Recent examples include Toys "R" Us and Shopko. For that reason, we have concerns about the spread and effect of private equity investment in many sectors of the economy, including the election technology industry—an integral part of our nation's democratic process. We are particularly concerned that secretive and "trouble-plagued companies," owned by private equity firms and responsible for manufacturing and maintaining voting machines and other election administration equipment, "have long skimped on security in favor of convenience," leaving voting systems across the country "prone to security problems." In light of these concerns, we request that you provide information about your firm, the portfolio

¹ Atlantic, "The Demise of Toys 'R' Us Is a Warning," Bryce Covert, July/August 2018 issue, https://www.theatlantic.com/magazine/archive/2018/07/toys-r-us-bankruptcy-private-equity/561758/; Axios, "How workers suffered from Shopko's bankruptcy while Sun Capital made money," Dan Primack, "How workers suffered from Shopko's bankruptcy while Sun Capital made money," June 11, 2019, https://www.axios.com/shopko-bankruptcy-sun-capital-547b97ba-901c-4201-92cc-6d3168357fa3.html.

² ProPublica, "The Market for Voting Machines Is Broken. This Company Has Thrived in It.," Jessica Huseman, October 28, 2019, https://www.propublica.org/article/the-market-for-voting-machines-is-broken-this-company-has-thrived-in-it.

³ Associated Press News, "US Election Integrity Depends on Security-Challenged Firms," Frank Bajak, October 28, 2019, https://apnews.com/f6876669cb6b4c4c9850844f8e015b4c.

companies in which it has invested, the performance of those investments, and the ownership and financial structure of your funds.

Over the last two decades, the election technology industry has become highly concentrated, with a handful of consolidated vendors controlling the vast majority of the market. In the early 2000s, almost twenty vendors competed in the election technology market. Today, three large vendors—Election Systems & Software, Dominion Voting Systems, and Hart InterCivic—collectively provide voting machines and software that facilitate voting for over 90% of all eligible voters in the United States. Private equity firms reportedly own or control each of these vendors, with very limited "information available in the public domain about their operations and financial performance." While experts estimate that the total revenue for election technology vendors is about \$300 million, there is no publicly available information on how much those vendors dedicate to research and development, maintenance of voting systems, or profits and executive compensation.

Concentration in the election technology market and the fact that vendors are often "more seasoned in voting machine and technical services contract negotiations" than local election officials, give these companies incredible power in their negotiations with local and state governments. As a result, jurisdictions are often caught in expensive agreements in which the same vendor both sells or leases, and repairs and maintains voting systems—leaving local officials dependent on the vendor, and the vendor with little incentive to substantially overhaul and improve its products. In fact, the Election Assistance Commission (EAC), the primary federal body responsible for developing voluntary guidance on voting technology standards, advises state and local officials to consider "the cost to purchase or lease, operate, and maintain a voting system over its life span ... [and to] know how the vendor(s) plan to be profitable" when signing contracts, because vendors typically make their profits by ensuring "that they will be around to maintain it after the sale." The EAC has warned election officials that "[i]f you do not manage the vendors, they will manage you."

Election security experts have noted for years that our nation's election systems and infrastructure are under serious threat. In January 2017, the U.S. Department of Homeland Security designated the United States' election infrastructure as "critical infrastructure" in order to prioritize the protection of our elections and to more effectively assist state and local election

⁴ Bloomberg, "Private Equity Controls the Gatekeepers of American Democracy," Anders Melin and Reade Pickert, November 3, 2018, https://www.bloomberg.com/news/articles/2018-11-03/private-equity-controls-the-gatekeepers-of-american-democracy.

⁵ Penn Wharton Public Policy Initiative, "The Business of Voting," July 2018, https://publicpolicy.wharton.upenn.edu/live/files/270-the-business-of-voting.

[°] Id

⁷ Id.

⁸ Brennan Center for Justice, "America's Voting Machines at Risk," Lawrence Norden and Christopher Famighetti, 2015, https://www.brennancenter.org/sites/default/files/publications/Americas Voting Machines At Risk.pdf; Penn Wharton Public Policy Initiative, "The Business of Voting," July 2018, https://publicpolicy.wharton.upenn.edu/live/files/270-the-business-of-voting.

⁹ U.S. Election Assistance Commission, "Ten Things to Know About Selecting a Voting System," October 14, 2017, https://www.eac.gov/documents/2017/10/14/ten-things-to-know-about-selecting-a-voting-system-cybersecurity-voting-systems-voting-technology/.

officials in addressing these risks. ¹⁰ However, voting machines are reportedly falling apart across the country, as vendors neglect to innovate and improve important voting systems, putting our elections at avoidable and increased risk. ¹¹ In 2015, election officials in at least 31 states, representing approximately 40 million registered voters, reported that their voting machines needed to be updated, with almost every state "using some machines that are no longer manufactured." ¹² Moreover, even when state and local officials work on replacing antiquated machines, many continue to "run on old software that will soon be outdated and more vulnerable to hackers." ¹³

In 2018 alone "voters in South Carolina [were] reporting machines that switched their votes after they'd inputted them, scanners [were] rejecting paper ballots in Missouri, and busted machines [were] causing long lines in Indiana." In addition, researchers recently uncovered previously undisclosed vulnerabilities in "nearly three dozen backend election systems in 10 states." And, just this year, after the Democratic candidate's electronic tally showed he received an improbable 164 votes out of 55,000 cast in a Pennsylvania state judicial election in 2019, the county's Republican Chairwoman said, "[n]othing went right on Election Day. Everything went wrong. That's a problem." These problems threaten the integrity of our elections and demonstrate the importance of election systems that are strong, durable, and not vulnerable to attack.

H.I.G. reportedly owns or has had investments in Hart InterCivic, a major election technology vendor. In order to help us understand your firm's role in this sector, we ask that you provide answers to the following questions no later than December 20, 2019.

- 1. Please provide the disclosure documents and information enumerated in Sections 501 and 503 of the Stop Wall Street Looting Act. 17
- 2. Which election technology companies, including all affiliates or related entities, does H.I.G. have a stake in or own? Please provide the name of and a brief description of the services each company provides.

¹⁰ Department of Homeland Security, "Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector," January 6, 2017,

https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical.

11 AP News, "US election integrity depends on security-challenged firms," Frank Bajak, October 29, 2018, https://apnews.com/f6876669cb6b4e4c9850844f8e015b4c; Penn Wharton Public Policy Initiative, "The Business of Voting," July 2018, https://publicpolicy.wharton.upenn.edu/live/files/270-the-business-of-voting.

¹² Brennan Center for Justice, "America's Voting Machines at Risk," Lawrence Norden and Christopher Famighetti, 2015, https://www.brennancenter.org/sites/default/files/publications/Americas Voting Machines At Risk.pdf.

¹³ Associated Press, "AP Exclusive: New election systems use vulnerable software," Tami Abdollah, July 13, 2019, https://apnews.com/e5e070c31f3c497fa9e6875f426ccde1.

¹⁴ Vice, "Here's Why All the Voting Machines Are Broken and the Lines Are Extremely Long," Jason Koebler and Manthew Gault, November 6, 2018, https://www.vice.com/en_us/article/59vzgn/heres-why-all-the-voting-machines-are-broken-and-the-lines-are-extremely-long.

¹³ Vice, "Exclusive: Critical U.S. Election Systems Have Been Left Exposed Online Despite Official Denials," Kim Zetter, August 8, 2019, https://www.vice.com/en_us/article/3kxzk9/exclusive-critical-us-election-systems-have-been-left-exposed-online-despite-official-denials.

New York Times, "A Pennsylvania Country's Election Day Nightmare Underscores Voting Machine Concerns," Nick Corasaniti, November 30, 2019, https://www.nytimes.com/2019/11/30/us/politics/pennsylvania-voting-machines.html.

¹⁷ Stop Wall Street Looting Act, S.2155, https://www.congress.gov/bill/116th-congress/senate-bill/2155.

- a. Which election technology companies, including all affiliates or related entities, has H.I.G. had a stake in or owned in the past twenty years? Please provide the name of and a brief description of the services each company provides or provided.
- b. For each election technology company H.I.G. had a stake in or owned in the past twenty years, including all affiliates or related entities, please provide the following information for each year that the firm has had a stake in or owned this company and the five years preceding the firm's investment.
 - i. The name of the company
 - ii. Ownership stake
 - iii. Total revenue
 - iv. Net income
 - v. Percentage of revenue dedicated to research and development
 - vi. Total number of employees
 - vii. A list of all state and local jurisdictions with which the company has a contract to provide election related products or services
 - viii. Other private-equity firms that own a stake in the company
- 3. Has any election technology company, including all affiliates or related entities, in which H.I.G. has an ownership stake or has had an ownership stake in the last twenty years, been found to have been in noncompliance with the EAC's Voluntary Voting System Guidelines? If so, please provide a copy of each EAC noncompliance notice received by the company and a description of what steps the company took to resolve each issue.
- 4. Has any election technology company, including all affiliates or related entities, in which H.I.G. has an ownership stake or has had an ownership stake in the last twenty years, been found to have been in noncompliance with any state or local voting system guidelines or practices? If so, please provide a list of all such instances and a description of what steps the company took to resolve each issue.
- 5. Has any election technology company, including all affiliates or related entities, in which H.I.G. has an ownership stake or has had an ownership stake in the last twenty years, been found to have violated any federal or state laws or regulations? If so, please provide a complete list, including the date and description, of all such violations.
- 6. Has any election technology company, including all affiliates or related entities, in which H.I.G. has an ownership stake or has had an ownership stake in the last twenty years, reached a settlement with any federal or state law enforcement entity related to a potential violation of any federal or state laws or regulations? If so, please provide a complete list, including the date and description, of all such settlements.

7. Has any election technology company, including all affiliates or related entities, in which H.I.G. has an ownership stake or has had an ownership stake in the past twenty years, reached a settlement with any state or local jurisdiction related to a potential violation of or breach of contract? If so, please provide a complete list, including the date and description, of all such settlements.

Thank you for your attention to this matter.

Sincerely,

Elizabeth Warren

United States Senator

Amy Klobuchar United States Senator

Ron Wyden

United States Senator

Mark Pocan

Member of Congress

Congress of the United States

Washington, DC 20510

December 6, 2019

Stephen D. Owens Managing Director Staple Street Capital Group, LLC

Hootan Yaghoobzadeh Managing Director Staple Street Capital Group, LLC

Dear Messrs. Owens and Yaghoobzadeh:

We are writing to request information regarding Staple Street Capital Group, LLC's (Staple Street) investment in Dominion Voting System (Dominion) one of three election technology vendors responsible for developing, manufacturing and maintaining the vast majority of voting machines and software in the United States, and to request information about your firm's structure and finances as it relates to this company.

Some private equity funds operate under a model where they purchase controlling interests in companies and implement drastic cost-cutting measures at the expense of consumers, workers, communities, and taxpayers. Recent examples include Toys "R" Us and Shopko. For that reason, we have concerns about the spread and effect of private equity investment in many sectors of the economy, including the election technology industry—an integral part of our nation's democratic process. We are particularly concerned that secretive and "trouble-plagued companies," owned by private equity firms and responsible for manufacturing and maintaining voting machines and other election administration equipment, "have long skimped on security in favor of convenience," leaving voting systems across the country "prone to security problems." In light of these concerns, we request that you provide information about your firm, the portfolio

Atlantic, "The Demise of Toys 'R' Us Is a Warning," Bryce Covert, July/August 2018 issue, https://www.theatlantic.com/magazine/archive/2018/07/toys-r-us-bankruptcy-private-equity/561758/; Axios, "How workers suffered from Shopko's bankruptcy while Sun Capital made money," Dan Primack, "How workers suffered from Shopko's bankruptcy while Sun Capital made money," June 11, 2019, https://www.axios.com/shopko-bankruptcy-sun-capital-547b97ba-901c-4201-92cc-6d3168357fa3.html.

² ProPublica, "The Market for Voting Machines is Broken. This Company Has Thrived in It.," Jessica Huseman, October 28, 2019, https://www.propublica.org/article/the-market-for-voting-machines-is-broken-this-company-has-thrived-in-it.

³ Associated Press News, "US Election Integrity Depends on Security-Challenged Firms," Frank Bajak, October 28, 2019, https://apnews.com/f6876669cb6b4e4c9850844f8e015b4c.

companies in which it has invested, the performance of those investments, and the ownership and financial structure of your funds.

Over the last two decades, the election technology industry has become highly concentrated, with a handful of consolidated vendors controlling the vast majority of the market. In the early 2000s, almost twenty vendors competed in the election technology market. Today, three large vendors—Election Systems & Software, Dominion, and Hart InterCivic—collectively provide voting machines and software that facilitate voting for over 90% of all eligible voters in the United States. Private equity firms reportedly own or control each of these vendors, with very limited "information available in the public domain about their operations and financial performance." While experts estimate that the total revenue for election technology vendors is about \$300 million, there is no publicly available information on how much those vendors dedicate to research and development, maintenance of voting systems, or profits and executive compensation.

Concentration in the election technology market and the fact that vendors are often "more seasoned in voting machine and technical services contract negotiations" than local election officials, give these companies incredible power in their negotiations with local and state governments. As a result, jurisdictions are often caught in expensive agreements in which the same vendor both sells or leases, and repairs and maintains voting systems—leaving local officials dependent on the vendor, and the vendor with little incentive to substantially overhaul and improve its products. In fact, the Election Assistance Commission (EAC), the primary federal body responsible for developing voluntary guidance on voting technology standards, advises state and local officials to consider "the cost to purchase or lease, operate, and maintain a voting system over its life span ... [and to] know how the vendor(s) plan to be profitable" when signing contracts, because vendors typically make their profits by ensuring "that they will be around to maintain it after the sale." The EAC has warned election officials that "[i]f you do not manage the vendors, they will manage you."

Election security experts have noted for years that our nation's election systems and infrastructure are under serious threat. In January 2017, the U.S. Department of Homeland Security designated the United States' election infrastructure as "critical infrastructure" in order to prioritize the protection of our elections and to more effectively assist state and local election

⁴ Bloomberg, "Private Equity Controls the Gatekeepers of American Democracy," Anders Melin and Reade Pickert, November 3, 2018, https://www.bloomberg.com/news/articles/2018-11-03/private-equity-controls-the-gatekeepers-of-american-democracy.

⁵ Penn Wharton Public Policy Initiative, "The Business of Voting," July 2018, https://publicpolicy.wharton.upenn.edu/live/files/270-the-business-of-voting.

⁷ Id.

Brennan Center for Justice, "America's Voting Machines at Risk," Lawrence Norden and Christopher Famighetti, 2015, https://www.brennancenter.org/sites/default/files/publications/Americas_Voting_Machines_At_Risk.pdf; Penn Wharton Public Policy Initiative, "The Business of Voting," July 2018, https://publicpolicy.wharton.upenn.edu/live/files/270-the-business-of-voting.

⁹ U.S. Election Assistance Commission, "Ten Things to Know About Selecting a Voting System," October 14, 2017, https://www.eac.gov/documents/2017/10/14/ten-things-to-know-about-selecting-a-voting-system-cybersecurity-voting-systems-voting-technology/.

officials in addressing these risks. ¹⁰ However, voting machines are reportedly falling apart across the country, as vendors neglect to innovate and improve important voting systems, putting our elections at avoidable and increased risk. ¹¹ In 2015, election officials in at least 31 states, representing approximately 40 million registered voters, reported that their voting machines needed to be updated, with almost every state "using some machines that are no longer manufactured." ¹² Moreover, even when state and local officials work on replacing antiquated machines, many continue to "run on old software that will soon be outdated and more vulnerable to hackers." ¹³

In 2018 alone "voters in South Carolina [were] reporting machines that switched their votes after they'd inputted them, scanners [were] rejecting paper ballots in Missouri, and busted machines [were] causing long lines in Indiana." In addition, researchers recently uncovered previously undisclosed vulnerabilities in "nearly three dozen backend election systems in 10 states." And, just this year, after the Democratic candidate's electronic tally showed he received an improbable 164 votes out of 55,000 cast in a Pennsylvania state judicial election in 2019, the county's Republican Chairwoman said, "[n]othing went right on Election Day. Everything went wrong. That's a problem." These problems threaten the integrity of our elections and demonstrate the importance of election systems that are strong, durable, and not vulnerable to attack.

Staple Street reportedly owns or has had investments in Dominion, a major election technology vendor. In order to help us understand your firm's role in this sector, we ask that you provide answers to the following questions no later than December 20, 2019.

- Please provide the disclosure documents and information enumerated in Sections 501 and 503 of the Stop Wall Street Looting Act. 17
- Which election technology companies, including all affiliates or related entities, does Staple Street have a stake in or own? Please provide the name of and a brief description of the services each company provides.

¹⁰ Department of Homeland Security, "Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector," January 6, 2017,

https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical.

11 AP News, "US election integrity depends on security-challenged firms," Frank Bajak, October 29, 2018, https://apnews.com/f6876669cb6b4e4c9850844f8e015b4c; Penn Wharton Public Policy Initiative, "The Business of

Voting," July 2018, https://publicpolicy.wharton.upenn.edu/live/files/270-the-business-of-voting.

Brennan Center for Justice, "America's Voting Machines at Risk," Lawrence Norden and Christopher Famighetti, 2015, https://www.brennancenter.org/sites/default/files/publications/Americas Voting Machines At Risk.pdf.

¹³ Associated Press, "AP Exclusive: New election systems use vulnerable software," Tami Abdollah, July 13, 2019,

https://apnews.com/e5e070c31f3c497fa9e6875f426ccde1.

¹⁴ Vice, "Here's Why All the Voting Machines Are Broken and the Lines Are Extremely Long," Jason Koebler and Matthew Gault, November 6, 2018, https://www.vice.com/en_us/article/59vzgn/heres-why-all-the-voting-machines-are-broken-and-the-lines-are-extremely-long.

¹⁵ Vice, "Exclusive: Critical U.S. Election Systems Have Been Left Exposed Online Despite Official Denials," Kim Zetter, August 8, 2019, https://www.vice.com/en_us/article/3kxzk9/exclusive-critical-us-election-systems-have-been-left-exposed-online-despite-official-denials.

¹⁶ New York Times, "A Pennsylvania Country's Election Day Nightmare Underscores Voting Machine Concerns," Nick Corasaniti, November 30, 2019, https://www.nytimes.com/2019/11/30/us/politics/pennsylvania-voting-machines.html.

¹⁷ Stop Wall Street Looting Act, S.2155, https://www.congress.gov/bill/116th-congress/senate-bill/2155.

- a. Which election technology companies, including all affiliates or related entities, has Staple Street had a stake in or owned in the past twenty years? Please provide the name of and a brief description of the services each company provides or provided.
- b. For each election technology company Staple Street had a stake in or owned in the past twenty years, including all affiliates or related entities, please provide the following information for each year that the firm has had a stake in or owned this company and the five years preceding the firm's investment.
 - i. The name of the company
 - ii. Ownership stake
 - iii. Total revenue
 - iv. Net income
 - v. Percentage of revenue dedicated to research and development
 - vi. Total number of employees
 - vii. A list of all state and local jurisdictions with which the company has a contract to provide election related products or services
 - viii. Other private-equity firms that own a stake in the company
- 3. Has any election technology company, including all affiliates or related entities, in which Staple Street has an ownership stake or has had an ownership stake in the last twenty years, been found to have been in noncompliance with the EAC's Voluntary Voting System Guidelines? If so, please provide a copy of each EAC noncompliance notice received by the company and a description of what steps the company took to resolve each issue.
- 4. Has any election technology company, including all affiliates or related entities, in which Staple Street has an ownership stake or has had an ownership stake in the last twenty years, been found to have been in noncompliance with any state or local voting system guidelines or practices? If so, please provide a list of all such instances and a description of what steps the company took to resolve each issue.
- 5. Has any election technology company, including all affiliates or related entities, in which Staple Street has an ownership stake or has had an ownership stake in the last twenty years, been found to have violated any federal or state laws or regulations? If so, please provide a complete list, including the date and description, of all such violations.
- 6. Has any election technology company, including all affiliates or related entities, in which Staple Street has an ownership stake or has had an ownership stake in the last twenty years, reached a settlement with any federal or state law enforcement entity related to a potential violation of any federal or state laws or regulations? If so, please provide a complete list, including the date and description, of all such settlements.

7. Has any election technology company, including all affiliates or related entities, in which Staple Street has an ownership stake or has had an ownership stake in the past twenty years, reached a settlement with any state or local jurisdiction related to a potential violation of or breach of contract? If so, please provide a complete list, including the date and description, of all such settlements.

Thank you for your attention to this matter.

Sincerely,

lizabeth Warren

Inited States Senator

now

Ron Wyden

United States Senator

Amy Klobuc ar United States Senator

Mark Pocan

Member of Congress



Home

Politics

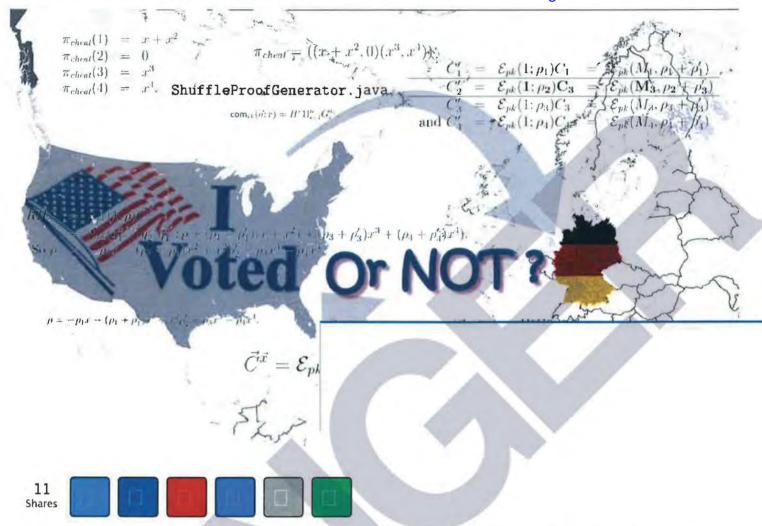
Commentary

Swiss and Aussies find a critical flaw in Scytl software that the US ignores

Commentary ◆ Featured ◆ Patriot Profiles by Jeanne McKinney ◆ Politics

Swiss and Aussies find a critical flaw in Scytl software that the US ignores

written by Jeanne McKinney Nov 18, 2020



SAN DIEGO: How is it the Swiss and Aussies were better positioned to handle voting than the U.S.? They vetted Scytl online voting software and discovered alarming features. Due diligence proved Scytl software not secure, not verifiable end to end. They must have known a bad electronic voting system could put the wrong candidate in office. They cared enough to prevent that from happening in their countries.

SwissPost intended to roll out an online voting system to "boost participation" and "deliver faster results than postal counts. Australia thought it could be more convenient, too. So, they contacted respected academics to dive into the software code.

Vanessa Teague, (professor at the University of Melbourne at the time) is known for her work on secret sharing, cryptographic protocols, and the security of electronic voting. Teague teamed up to evaluate Scytl with an international group of researchers.

They published a report on March 12, 2019, called "The use of trapdoor commitments in Bayer-Groth proofs and he implications for the verifiability of the Scytl-SwissPost Internet voting system*"

The researchers probed the "shuffling and decryption components of Switzerland's online voting system." Their 'act relevant to New South Wales' iVote online system because both were developed by Scytl, a company headquartered in Barcelona [and Frankfurt] that specializes in secure electronic voting," says InnovationAus.

Attorney Sidney Powell: Protecting America from hacked voting software

Aussies, Swiss found back door to future election disaster.

Online or mail-in voting may seem like a solution to a world trying to survive a raging COVID-19 pandemic. But without thorough vetting – it's like giving criminal minds a gun AND the ammunition. When you send an electronic vote it's floating through nebulous, unquantified cyberspace. It may solve getting to the polls in a physical sense and getting votes counted quickly. But it doesn't change the challenges of control of information.

On Mar 12, 2019, MIT published a technology review on the Scytl research, "A cryptographic trap door could let someone change votes cast using Switzerland's online sVote system without being detected, according to a new paper."

Vice News reported same day,

"The cryptographic backdoor exists in a part of the system that is supposed to verify that all of the ballots and votes counted in an election are the same ones that voters cast. But the flaw could allow someone to swap out all of the legitimate ballots and replace them with fraudulent ones, all without detection," says Vice.

"The vulnerability is astonishing," said Matthew Green, who teaches cryptography at Johns Hopkins University and did not do the research but read the researchers' report. "In normal elections, there is no single person who could undetectably defraud the entire election. But in this system they built, there is a party who could do that," adds Vice.



11,354 Votes



Lawyer Sidney Powell: Democrats used Dominion machines to steal votes

As best understood by this writer, the researchers said they couldn't state one way or the other if Scytl was less than expert at what they do or if they purposely created exploitable flaws. They are clear that the software is flawed and can be hacked. They state that it would be a good cover to write immature code which attempts to follow a published encryption method and that their flawed implementation could more easily be forgiven for doing so.

Or was the revealed flaw a feature for nefarious use?

The academic research asserts that Scytl followed the Bayer – Groth encryption method. Although they general collowed the algorithm, they say Scytl failed to protect key pieces of data. They also said the data can be hacked, changing votes without a trace.

You would need to be expert in the algorithm to understand the specific critiques in the paper.

Election stealing issue in Scytl-SwissPost Internet voting system.

"Verifiability is a critical part of the trustworthiness of e-voting systems. Universal verifiability means that a proof of proper election conduct should be verifiable by any member of the public," says the report.

"This mixnet has a trapdoor – a malicious administrator or software provider for the mix could manipulate votes but produce a proof transcript that passes verification. Thus complete verifiability fails," concludes the researchers.

Sarah Jamie Lewis (former computer scientist for British Government Communications Headquarters (GCHQ) intelligence agency) was a critical member of the team. She says, "No election system should have a backdoor that allows the people running the election the ability to undetectably modify the election outcome...



"We have only examined a tiny fraction of this code base and found a critical, election-stealing issue," says Lewis.

Where was U.S. security, oversight for the 2020 Election?

"SwissPost, Switzerland's national postal service, published its shuffling and decryption code six months before it intended to use it for an election so that researchers like Professor Teague and colleague Lewis could vet the system for flaws," says InnovationAus. Olivier Pereira was also on the research team.

'indings led researchers to recommend the Swiss government immediately halt plans to implement the system more widely. But it was bigger than Switzerland. Scytl provides electronic voting services to 35 countries, (including the U.S.)

Case 1:21-cv-00317-DCLC-CHS Document 22-7 Filed 01/20/22 Page 226 of 591 PageID

Scytl said it was working on the Swiss [evote] flaw. That it managed to creep into the system in the first place worried MIT reviewers. The outcome is unknown. Scytl's statement on Swiss online major flaw.

We now know Scytl software cycled millions of U.S. votes. Lawyers work relentlessly to find out how many were modified in the 2020 election.

George Orwell's dystopian 1984 arrives in 2020: RIP America

Hackers could kick back and say 'who do you want to win'?

Russ Ramsland, Co-owner Allied Security Operations Group, was interviewed days leading up to the election. Excerpts about his findings:

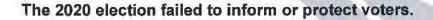


"There are no [U.S.] national security standards that a voting company needs to meet. The software is so bad, you can easily change the audit trail, so later you cannot forensically go back and find out the votes that were changed," says Ramsland.

"What happens to your vote after whatever the local voting company does to it? It turns out in the case of Texas and 27 other states – it goes to a [Scytl] server in Frankfurt Germany, owned by Barcelona Spain Multinational and that's actually who controls and reports your vote," he clarified.

So your vote in Texas or anywhere in 28 states (including battleground) connects you to some foreign power. Were voters informed of this chicanery or allowed consent to this? Of course not, the perpetrators thought it would remain hidden.

Ramsland said they could see malware collecting credentials of county workers who submit voting information up, allowing a bad actor to go back into the county and change votes not just in Frankfurt, but the U.S. too.



Our understanding of reality is changed each day by Trump's lawyers and legal helpers, headed up by tireless Sidney Powell. They will certainly prove in court Scytl software a very bad risk, like the Swiss and Aussies. They will dig deep to find those bad actors. Hats off to all who took the hard steps to report election fraud. Keep stepping.

If voters knew on November 3rd what we now know, there would have been no election.

Americans' trust in electronic voting systems has been blown to smithereens. This scheme to wipe out Trump's legitimate votes is massive, complex, and unAmerican. Truth, the most powerful force, lies with the president and his allies searching for the monsters defiling the 2020 election. Yet alas, "The Kraken," is here to fight.

Breaking news: Huge win for Trump in Michigan.



Featured Image:

Composite Artwork Dave McKinney

United States in North America Map TUBS https://commons.wikimedia.org/wiki/File:United_States_in_North_America_(-mini_map_-rivers).svg

Flag Map of Germany David Liuzzo and AxG https://commons.wikimedia.org/wiki/File:Flag_map_of_Germany.svg

Curved Arrow Amada44 https://commons.wikimedia.org/wiki/File:Curved_Arrow.svg Germany in Europe TUBS https://commons.wikimedia.org/wiki/File:Germany_in_Europe.svg

I Voted Sticker Dwight Burdette https://commons.wikimedia.org/wiki/File:I_Voted_Sticker.JPG

Math Formulas Sarah Jamie Lewis, Olivier Pereira, and Vanessa Teague https://people.eng.unimelb.edu.au/vjteague/UniversalVerifiabilitySwissPost.pdf



SPONSORED CONTENT ON CDN

\$10 Welcome Bonus!

\$10 Welcome Bonus!

By Rakuten

From The Web



According To CGI, This Is What Historical Figures Really Looked Like

Taco Relish



The Israeli-made face mask Everyone Is Talking About in the US

The Jerusalem Post

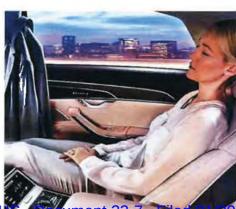


Sponsored Links by Taboola

Maps That Show Us A New Perspective

Explored Planet







case 1.21-cv-00317-DCLC-CHS D0cument 22-7 Filed 01/20/2z Page 230 01/591 Pager

#: 1788

The Real Reason Why Many Dogs Live Only Average of 9 Years

Ultimate Pet Nutrition Nutra Thrive

These Cars Are So Loaded It's Hard to Believe They're So Cheap

Luxury SUVs | Search Ads

These Aircraft Paint Jobs Are The Stuff Of Dreams

Yeah Motor















AUSSIE

SCYTL

SOFTWARE FLAW

SWISS

VOTING

0 comment

1



JEANNE MCKINNEY

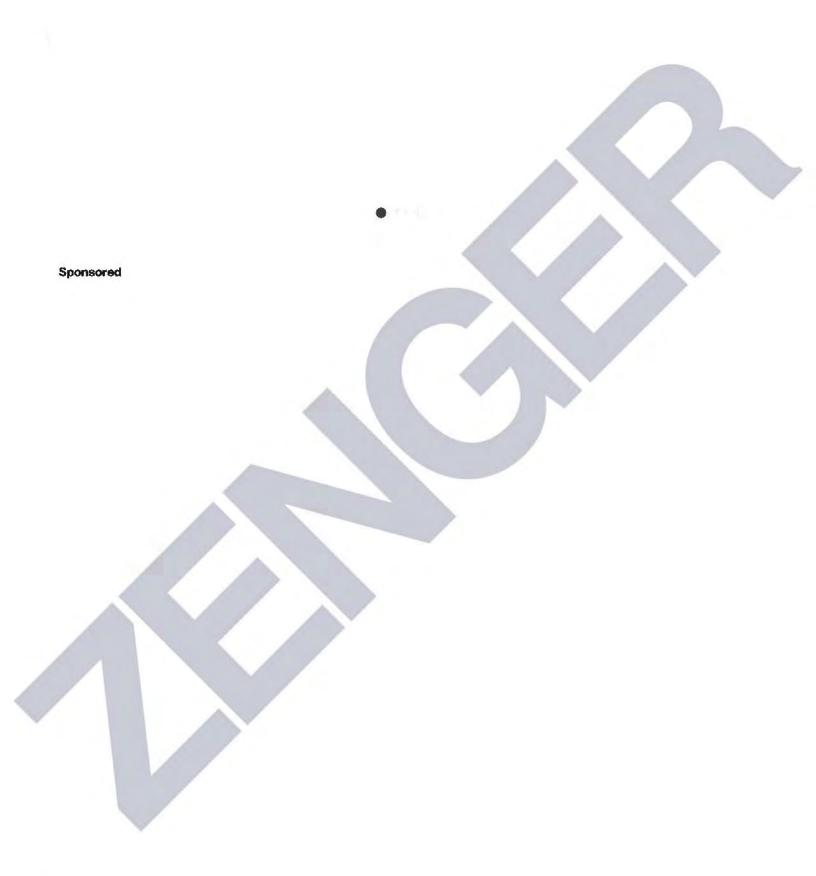
Jeanne McKinney is an award-winning writer whose focus and passion is our United States active-duty military members and military news. Her Patriot Profiles offer an inside look at the amazing active-duty men and women in all Armed Services, including U.S. Marine Corps, Navy, Army, Air Force, Coast Guard, and National Guard. Reporting includes first-hand accounts of combat missions in Iraq and Afghanistan, the fight against violent terror groups, global defense, tactical training and readiness, humanitarian and disaster relief assistance, next-generation defense technology, family survival at home, U.S. port and border protection and illegal interdiction, women in combat, honoring the Fallen, Wounded Warriors, Military Working Dogs, Crisis Response, and much more. McKinney has won twelve San Diego Press Club "Excellence in Journalism Awards", including seven First Place honors.

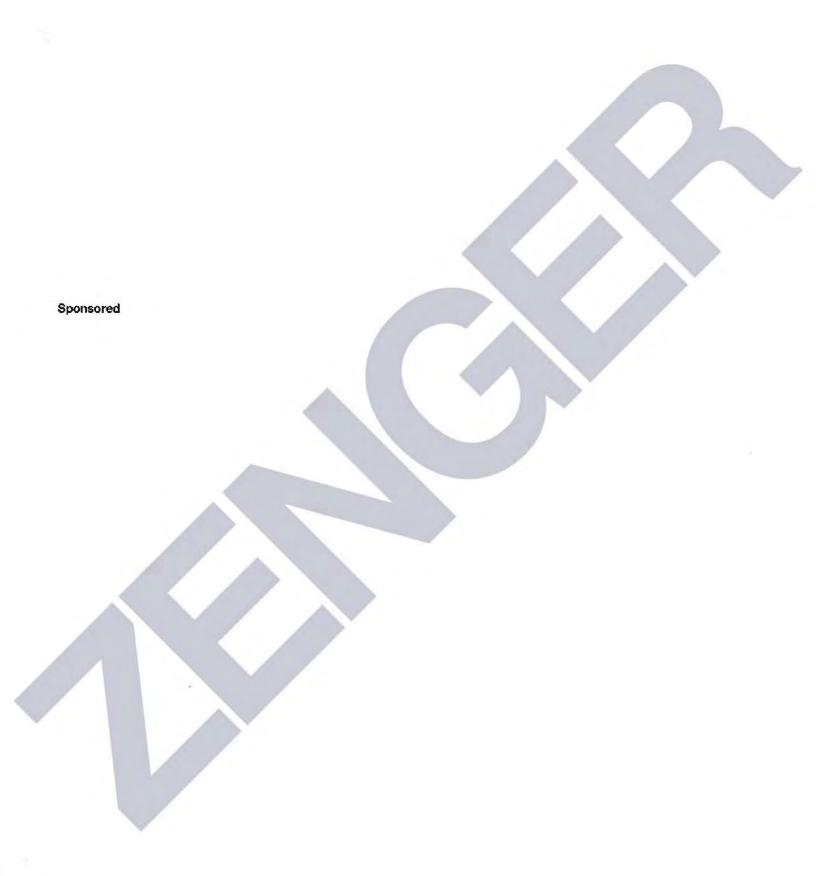
previous post

next post

George Orwell's dystopian 1984 arrives in 2020: RIP America

Lt. Gen McInerney enters the voter fray: Dems used Intelligence software







Type and hit enter...

KEEP IN TOUCH

Case 1:21-cv-00040 Document 1-114 Filed 01/08/21 Page 19 of 60

☐ FACEBOOK

TWITTER

□ INSTAGRAM

☐ PINTEREST

☐ LINKEDIN

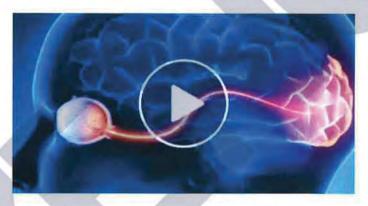


Which president did more to protect our 2nd Amendment rights? (Free Gift For All Who Answer)

Obama

Trump

1,842 Votes



Big Pharma Doesn't Want You To Know About This Eyesight Trick

36,067





Who do you trust more?

President Trump | Doctor Fauci



	ARIZONA	GEORGIA	MICHIGAN	NEVADA	PENNSYLVANIA	WISCO
ight Voter Fraud	1	1	*	1	*	V
ot Mishandling		V	1	V	✓	V
estable Process s	1	~	1	V	V	V
l Protection Clause tions	1	V	✓	V	✓	V
ig Machine ularities	1	1	√	V	1	*
ificant Statistical nalies	1	V	1	1		V
n "Victory" Margin	10,457	11,779	154,188	33,596	81,660	20,6
ible Illegal Ballots	>100,000	>400,000	Unknown	>100,000	>600,000	>200,

The Coup of America: Navarro says election was theft by a thousand cuts

1960's Nixon vs. Kennedy guide Congress on overturning election fraud

Knowing software would swap votes, did Dems choose Dominion?

Canelo vs Smith: Feliz Navidad for boxing fans Saturday

Big Drama Show hits blackjack: Golovkin sets record with 21st title defense Friday

AL GOODWYN CARTOONS

Al Goodwyn Cartoon: All is calm, no left anarchist too bright Al Goodwyn Cartoon: The Democrat Parties new face? Is it time for Joe Biden and Kamala Harris to consider conceding? Veterans Day 2020: A time to honor our vets, present and past Americans need Congress to pass "The New Voting Rights Act" **POPULAR POSTS** The 2015 Tour de France - Race Slideshow

President George Washington warns against political divisiveness

Jack is Back: Halloween Horror Nights at Universal Orlando

USEFUL LINKS

Contact

Privacy Policy

Cookie Policy

Media / Advertising

Who We Are / Masthead

Write for CommDigiNews

JommDigiNews Writer Directory

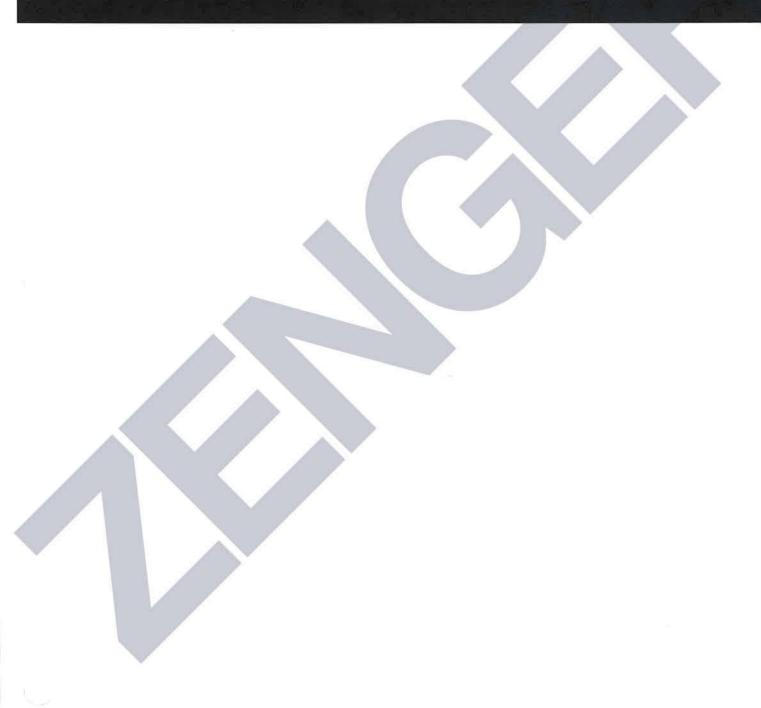
STORY CALENDAR

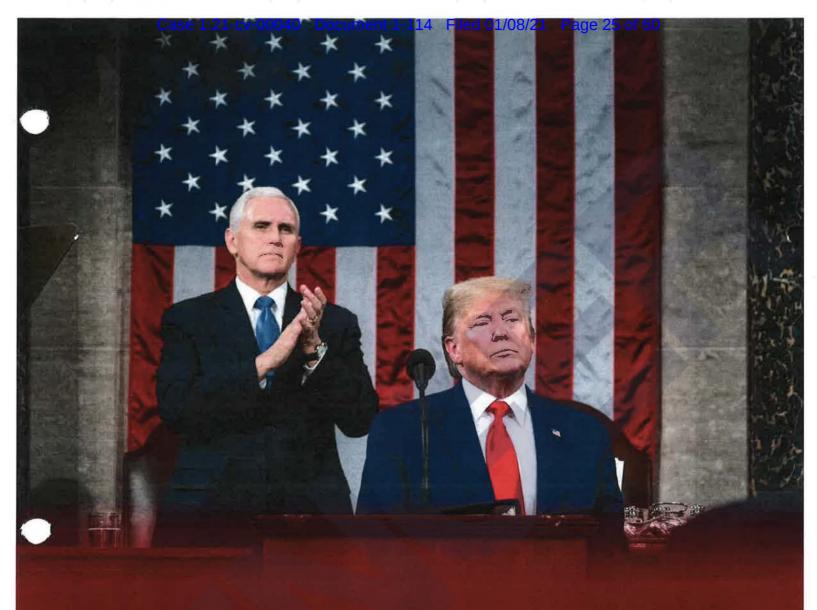
		9			D	ecember 2020
М	T	w	т	F	S	s
15	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

« Nov

©2017. Communities Digital News, LLC. The opinions of the author are their own.

The author and Communities Digital News owns the whole copy write of this article and it may not be duplicated without express permission.





THE IMMACULATE DECEPTION:

Six Key Dimensions of Election Irregularities

Executive Summary

This report assesses the fairness and integrity of the 2020 Presidential Election by examining six dimensions of alleged election irregularities across six key battleground states. Evidence used to conduct this assessment includes more than 50 lawsuits and judicial rulings, thousands of affidavits and declarations, testimony in a variety of state venues, published analyses by think tanks and legal centers, videos and photos, public comments, and extensive press coverage.

The matrix below indicates that significant irregularities occurred across all six battleground states and across all six dimensions of election irregularities. This finding lends credence to the claim that the election may well have been stolen from President Donald J. Trump.



From the findings of this report, it is possible to infer what may well have been a coordinated strategy to effectively stack the election deck against the Trump-Pence ticket. Indeed, the observed patterns of election irregularities are so consistent across the six battleground states that they suggest a coordinated strategy to, if not steal the election outright, strategically game the election process in such a way as to "stuff the ballot box" and unfairly tilt the playing field in favor of the Biden-Harris ticket. Topline findings of this report include:

- The weight of evidence and patterns of irregularities are such that it is irresponsible for anyone especially the mainstream media to claim there is "no evidence" of fraud or irregularities.
- The ballots in question because of the identified election irregularities are more than sufficient to swing the outcome in favor of President Trump should even a relatively small portion of these ballots be ruled illegal.

- All six battleground states exhibit most, or all, six dimensions of election irregularities.
 However, each state has a unique mix of issues that might be considered "most important."
 To put this another way, all battleground states are characterized by the same or similar election irregularities; but, like Tolstoy's unhappy families, each battleground state is different in its own election irregularity way.
- This was theft by a thousand cuts across six dimensions and six battleground states rather than any one single "silver bullet" election irregularity.
- In refusing to investigate a growing number of legitimate grievances, the anti-Trump media and censoring social media are complicit in shielding the American public from the truth. This is a dangerous game that simultaneously undermines the credibility of the media and the stability of our political system and Republic.
- Those journalists, pundits, and political leaders now participating in what has become a
 Biden Whitewash should acknowledge the six dimensions of election irregularities and
 conduct the appropriate investigations to determine the truth about the 2020 election. If
 this is not done before Inauguration Day, we risk putting into power an illegitimate and
 illegal president lacking the support of a large segment of the American people.
- The failure to aggressively and fully investigate the six dimensions of election irregularities
 assessed in this report is a signal failure not just of our anti-Trump mainstream media and
 censoring social media but also of both our legislative and judicial branches.
 - Republican governors in Arizona and Georgia together with Republican majorities in both chambers of the State Legislatures of five of the six battleground states Arizona, Georgia, Michigan, Pennsylvania, and Wisconsin² have had both the power and the opportunity to investigate the six dimensions of election irregularities presented in this report. Yet, wilting under intense political pressure, these politicians have failed in their Constitutional duties and responsibilities to do so and thereby failed both their states and this nation as well as their party.
 - O Both State courts and Federal courts, including the Supreme Court, have failed the American people in refusing to appropriately adjudicate the election irregularities that have come before them. Their failures pose a great risk to the American Republic.
- If these election irregularities are not fully investigated prior to Inauguration Day and thereby effectively allowed to stand, this nation runs the very real risk of never being able to have a fair presidential election again with the down-ballot Senate races scheduled for January 5 in Georgia an initial test case of this looming risk.

I. Introduction

At the stroke of midnight on Election Day, President Donald J. Trump appeared well on his way to winning a second term. He was already a lock to win both Florida and Ohio; and no Republican has ever won a presidential election without winning Ohio while only two Democrats have won the presidency without winning Florida.³

At the same time, the Trump-Pence ticket had substantial and seemingly insurmountable leads in Georgia, Pennsylvania, Michigan, and Wisconsin. If these leads held, these four key battleground states would propel President Trump to a decisive 294 to 244 victory in the Electoral College.

Shortly after midnight, however, as a flood of mail-in and absentee ballots began entering the count, the Trump red tide of victory began turning Joe Biden blue. As these mail-in and absentee ballots were tabulated, the President's large leads in Georgia, Pennsylvania, Michigan, and Wisconsin simply vanished into thin Biden leads.

At midnight on the evening of November 3, and as illustrated in Table 1, President Trump was ahead by more than 110,000 votes in Wisconsin and more than 290,000 votes in Michigan. In Georgia, his lead was a whopping 356,945; and he led in Pennsylvania by more than half a million votes. By December 7, however, these wide Trump leads would turn into razor thin Biden leads – 11,779 votes in Georgia, 20,682 votes in Wisconsin, 81,660 votes in Pennsylvania, and 154,188 votes in Michigan.

Table 1: A Trump Red Tide Turns Biden Blue

	GEORGIA	PENNSYLVANIA	MICHIGAN	WISCONSIN
Trump Lead Midnight 11/3	356,945	555,189	293,052	112,022
Biden "Lead" 12/15	11,779	81,660	154,188	20,682

There was an equally interesting story unfolding in Arizona and Nevada. While Joe Biden was ahead in these two additional battleground states on election night – by just over 30,000 votes in Nevada and less than 150,000 votes in Arizona – internal Trump Campaign polls predicted the President would close these gaps once all the votes were counted. Of course, this never happened.

In the wake of this astonishing reversal of Trump fortune, a national firestorm has erupted over the fairness and integrity of one of the most sacrosanct institutions in America – our presidential election system. Critics on the Right and within the Republican Party – including President Trump himself – have charged that the election was stolen. They have backed up these damning charges with more than 50 lawsuits,⁴ thousands of supporting affidavits and declarations, and seemingly incriminating videos, photos, and first-hand accounts of all manner of chicanery.⁵

Critics on the Left and within the Democrat Party have, on the other hand, dismissed these charges as the sour grapes of a whining loser. Some of these critics have completely denied any fraud, misconduct or malfeasance altogether. Others have acknowledged that while some election irregularities may have existed, they strenuously insist that these irregularities are not significant enough to overturn the election.

There is a similar Battle Royale raging between large anti-Trump segments of the so-called "mainstream" media and alternative conservative news outlets. Across the anti-Trump mainstream media diaspora – which includes most prominently print publications like the New York Times and Washington Post and cable TV networks like CNN and MSNBC – a loud chorus of voices has been demanding that President Trump concede the election.

These same anti-Trump voices have been equally quick to denounce or discredit anyone – especially anyone within their own circle – that dares to investigate what may well turn out to be THE biggest political scandal in American history. Social media outlets like Facebook, Twitter, and YouTube likewise have been actively and relentlessly censoring anyone who dares to call the results of the election into question.

In contrast, alternative news outlets, primarily associated with the American conservative movement, have provided extensive, in-depth coverage of the many issues of fraud, misconduct, and other irregularities that are coming to light. From Steve Bannon's War Room Pandemic⁶ and John Solomon's Just the News¹ to Raheem Kassam's National Pulse, to Newsmax, and One America News Network, Americans hungry for facts and breaking developments have been able to find such critical information only by following this alternative coverage.

That the American public is not buying what the Democrat Party and the anti-Trump media and social media are selling is evident in public opinion polls. For example, according to a recent Rasmussen poll: "Sixty-two percent (62%) of Republicans say it is 'Very Likely the Democrats stole the election'" while 28% of Independents and 17% of Democrats share that view.¹¹

If, in fact, compelling evidence comes to light proving the election was indeed stolen after a *fait* accompli Biden inauguration, we as a country run the very real risk that the very center of our great American union will not hold.

To put this another way, if the greatest democracy in world history cannot conduct a free and fair election, and if much of the mainstream media of this country won't even fully investigate what is becoming a growing mountain of evidence calling into question the election result, there is little chance that our democracy and this Republic will survive as we know it. It is therefore critical that we get to the bottom of this matter. That is the purpose of this report.

II. Six Dimensions of Election Irregularities across Six Battleground States

This report assesses the fairness and integrity of the 2020 presidential election across six key battleground states where the Democrat candidate Joe Biden holds a slim lead, and the results continue to be hotly contested. As documented in the extensive endnotes, the evidence used to conduct this assessment includes more than 50 lawsuits and judicial rulings, thousands of affidavits and declarations, testimony presented in a variety of state venues, published reports and analyses by think tanks and legal centers, videos and photos, public comments and first-hand accounts, and extensive press coverage.

From a review and analysis of this evidence, six major dimensions of alleged election irregularities have been identified and assessed on a state-by-state basis across six key battleground states: Arizona, Georgia, Michigan, Nevada, Pennsylvania, and Wisconsin. These six dimensions include outright voter fraud, ballot mishandling, contestable process fouls, Equal Protection Clause violations, voting machine irregularities, and significant statistical anomalies.

The matrix in Table 2 provides an overview of the presence or absence of each of the six dimensions of alleged election irregularities in each of the six battleground states. Column 1 lists each of the six dimensions along with the alleged Biden victory margin and the possible illegal ballots due to election irregularities. Columns 2 through 7 in the matrix then indicate the presence or absence of the election irregularities in any given state.

Note that a checkmark in matrix cell indicates there is *widespread* evidence in a given state for a particular dimension of election irregularity while a star indicates there is at least *some* evidence.

ARIZONA MICHIGAN NEVADA PENNSYLVANIA WISCONSIN GEORGIA **Outright Voter Fraud Ballot Mishandling Contestable Process Fouls Equal Protection Clause Violations Voting Machine** Irregularities Significant Statistical **Anomalies** 81,660 20,682 Biden "Victory" Margin 10,457 11,779 154,188 33,596 >100,000 >400,000 Unknown >100,000 >600,000 >200,000 **Possible Illegal Ballots**

Table 2: 2020 Alleged Election Irregularities across the Six Battleground States

= Wide-Spread Evidence * = Some Evidence

Two key points stand out immediately from the matrix. First, significant irregularities appear to be ubiquitous across the six battleground states. Only Arizona is free of any apparent widespread ballot mishandling while only Pennsylvania lacks significant statistical anomalies. The rest of the matrix in Table 2 is a sea of checkmarks and occasional stars.

Second, if one compares the alleged Biden victory margin in Column 7 of the figure with the possible illegal ballots in Column 8, it should be clear that the number of possible illegal ballots dwarfs the alleged Biden victory margin in five of the six states.

For example, the alleged Biden victory margin in Nevada is 33,596 votes yet the number of ballots in question is more than three times that. In Arizona, which has the narrowest alleged Biden victory margin at 10,457 votes, there are nearly 10 times that number of possible illegal ballots; and the ratio of the alleged Biden vote lead to possible illegal ballots is even higher for Georgia.

Only Michigan is the exception to the rule. This is not because it is likely to be a true exception but simply because there remains insufficient estimates of how the various types of irregularities in Michigan translate into possible illegal votes.

Clearly, based on this matrix, the American people deserve a definitive answer as to whether this election was stolen from Donald J. Trump. Absent a thorough investigation prior to Inauguration Day, a cloud and a stain will hang over what will be perceived by many Americans as an illegitimate Biden administration.

The next six sections of this report examine in more detail each of the six dimensions of alleged election irregularities.

III. Outright Voter Fraud

Outright voter fraud ranges from the large-scale manufacturing of fake ballots, bribery, and dead voters to ballots cast by ineligible voters such as felons and illegal aliens, ballots counted multiple times, and illegal out-of-state voters. Table 3 provides an overview across the six battleground states of the various types of outright voter fraud that have been alleged to be present.

PENNSYLVANIA ARIZONA GEORGIA MICHIGAN NEVADA WISCONSIN Bribery Fake Ballot Manufacturing & Destruction of Legally Cast Real Indefinitely Confined Voter **Abuses** Ineligible Voters & Voters Who Voted in Multiple States Dead Voters & Ghost Voters Counting Ballots Multiple Times Illegal Out-of-State Voters = Wide-Spread Evidence * = Some Evidence

Table 3: Outright Voter Fraud in the 2020 Presidential Election

From the figure, we see that different types of fraud may be present in all six states. Let's more precisely define each of these different types of fraud using examples that are designed to be illustrative rather than exhaustive.

Bribery

In a voter fraud context, *bribery* refers to the corrupt solicitation, acceptance, or transfer of value in exchange for official action, such as voter registration or voting for a preferred candidate. ¹² At least in Nevada, there is a slam dunk case that such bribery occurred.

What is so stunning about the Nevada case is the brazen disregard for our federal bribery laws. In the Silver State, in an effort orchestrated by the Biden campaign, Native Americans appear to have traded their votes not for pieces of silver but rather for Visa gift cards, jewelry, and other "swag." According to the Epoch Times, such vote buying schemes also may have occurred in eight other states, including Arizona and Wisconsin. 14

Fake Ballot Manufacturing and Destruction of Legally Cast Real Ballots

Fake ballot manufacturing involves the fraudulent production of ballots on behalf of a candidate; and one of the most disturbing examples of possible fake ballot manufacturing involves a truck driver who has alleged in a sworn affidavit that he picked up large crates of ballots in New York and delivered them to a polling location in Pennsylvania. ¹⁵ There may be well over 100,000 ballots involved, enough fake ballots alone to have swung the election to Biden in the Keystone State.

Likewise in Pennsylvania, there is both a Declaration and a photo that suggests a poll worker used an unsecured USB flash drive to dump an unusually large cache of votes onto vote tabulation machines. The resultant tabulations did not correlate with the mail-in ballots scanned into the machines. ¹⁶

Arguably the most flagrant example of possible fake ballot manufacturing on behalf of Joe Biden may have occurred at the State Farm Arena in Atlanta, Georgia. The possible perpetrators were caught *in flagrante delicto* on surveillance video.

In one version of this story, poll watchers and observers as well as the media were asked to leave in the middle of the night after a suspicious water leak. Once the room was cleared, several election officials pulled out large boxes of ballots from underneath a draped table. They then proceeded to tabulate a quantity of fake manufactured ballots estimated to be in the range of tens of thousands.¹⁷ Note that a large surge in Biden votes following the tabulation of these ballots can be clearly observed after these votes were processed.¹⁸

Despite what appears to be damning evidence of a possible crime, a spate of stories appeared across the anti-Trump media diaspora dismissing any concerns. According to these whitewash stories, these were regular and authorized ballot boxes, observers in the media were not asked to leave but simply left on their own, and it is perfectly acceptable to count ballots in the absence of observers. ¹⁹ Or so the spin goes.

Of course, this is precisely the kind of incident that should be fully investigated both by Georgia's Attorney General as well as by the Federal Department of Justice. Yet it remains unclear as to whether such investigations are underway. Meanwhile, the videotape itself, absent an adequate explanation, has contributed to the current climate of skepticism surrounding the fairness and integrity of the election.

Finally, as an example of the possible destruction of legally cast real ballots there is this allegation from a court case filed in the United States District Court for the District of Arizona: Plaintiffs claim that over 75,000 absentee ballots were reported as unreturned when they were actually returned. These absentee ballots were then either lost or destroyed (consistent with allegations of Trump ballot destruction) and/or were replaced with blank ballots filled out by election workers or other third parties.²⁰

Indefinitely Confined Voter Abuses

Indefinitely confined voters are those voters unable to vote in person because of old age or some disability. There are two types of possible abuses associated with such indefinitely confined voters.

The first kind of abuse involves exploiting the elderly or the infirm by effectively hijacking their identities and votes. For example, in Georgia, the family of an elderly man in a nursing home facility discovered that a mail-in ballot had been requested and submitted under his voter registration identity, yet it was done without his consent.²¹ In a similar situation in Pennsylvania, two parents and their daughter who has Downs Syndrome went to vote in person and discovered that a mail-in ballot had both been requested and submitted for the daughter without her consent.²²

The second kind of indefinitely confined voter abuse is far more consequential, at least in the state of Wisconsin. The key allegation here in several court filings is that "bad-faith voters" registering as "indefinitely confined" intentionally broke "Wisconsin election law to circumvent election integrity photo identification requirements." In a nutshell, they were able to vote without showing a voter identification photo and therefore underwent a far less rigorous I.D. check than would otherwise have been conducted.

This abuse happened, according to one press account, after "clerks in Dane and Milwaukee counties offered illegal advice that encouraged individuals to use indefinite confinement as a way to ignore the state's photo I.D. requirement." The Trump side has called this correctly an open invitation to fraud; and stories and pictures abound of Wisconsin voters who registered as indefinitely confined but were seen also attending weddings, riding their bikes, going on vacation, and otherwise be anything but confined. 24

Here is what is most important about this particular type of election fraud: In the wake of the expanded definition of indefinitely confined voters – a definition ruled legally *incorrect* by the Wisconsin Supreme Court²⁵ – the number of indefinitely confined voters surged from just under 70,000 voters in 2019 to over 200,000 in 2020.²⁶ This 130,000 vote increment of new indefinitely confined voters is more than five times the Biden victory margin in Wisconsin.

Ineligible Voters and Voters Who Voted in Multiple States

Ineligible voters include felons deemed ineligible, underage citizens, nonregistered voters, illegal aliens, illegal out-of-state voters, and voters illegally using a post office box as an address.²⁷

In a court filing by the Trump campaign legal team, lead counsel Ray Smith provided a list of more than 70,000 allegedly ineligible voters casting ballots in Georgia in the 2020 election. Also in Georgia, over 20,000 people appear to have filed a Notice of Changed Address form to the Georgia state government or had other indications of moving out of state. Yet, these clearly ineligible out-of-state voters appeared to have remained on the voter rolls and voted in the 2020 election. ²⁹

As additional data points regarding ineligible out-of-state voters, there are these: Between 80 and 100 self-proclaimed Black Lives Matter-affiliated members from other states have admitted to having voted in Pennsylvania.³⁰

As for those *voters who vote in multiple states*, one lawsuit claims that roughly 15,000 mail-in or absentee ballots were received in Nevada from voters who were known to have voted in other states.³¹ It is useful to note here that in Nevada, poll workers allegedly were not consistent in their procedures when checking voters in to vote about whether they accepted California or Nevada Voter Identification as proof of eligibility to register to vote.³²

Dead Voters and Ghost Voters

According to widespread evidence, there was a surprising number of ballots cast across several key battleground states by deceased voters, sparking one wag to quip, in reference to a classic Bruce Willis movie, this was the "Sixth Sense" election – I see dead people voting.

In Pennsylvania, for example, a statistical analysis conducted by the Trump Campaign matching voter rolls to public obituaries found what appears to be over 8,000 confirmed dead voters successfully casting mail-in ballots.³³ In Georgia – underscoring the critical role any given category of election irregularities might play in determining the outcome – the estimated number of alleged deceased individuals casting votes almost exactly equals the Biden victory margin.

In Michigan, according to one first-hand account offered in a declaration, computer operators at a polling location in Detroit were manually adding the names and addresses of thousands of ballots to vote tabulation systems with voters who had birth dates in 1900.³⁴ And in Nevada, a widower since 2017 saw that his deceased wife had successfully cast a mail-in ballot on November 2, 2020, three and a half years after her death. ³⁵

It may be useful to note here that dead voters played a critical role in stealing the election from Richard Nixon, a theft orchestrated by Mayor Richard Daley and his Chicago political machine. According to one report "more than 3,000 votes [were] cast in the names of individuals who were dead, and more than 31,000 individuals voted twice in different locations in the city." President Kennedy's victory margin in Illinois was less than 9,000 votes.

On the Ghost Voter front, a "Ghost Voter" is a voter who requests and submits a ballot under the name of a voter who no longer resides at the address where that voter was registered. In Georgia for example, it is alleged that over 20,000 absentee or early voters – almost twice the Biden victory margin – cast their ballots after having moved out of state. In Nevada, a poll worker reported that there were as many as 50 ballots per day being delivered to homes vacated by their former residents. The state of th

Counting Ballots Multiple Times

Counting ballots multiple times occurs most egregiously when batches of ballots are repeatedly rescanned and re-tabulated in electronic voting machines. It can also happen when the same person votes multiple times within the same day. Evidence of these particular kinds of "ballot stuffing" are present across all six battleground states.

For example, in Wisconsin, poll workers were observed running ballots through tabulation machines more than once.³⁸ In Wayne County, Michigan, Republican poll watchers observed canvassers re-scanning batches of ballots through vote tabulation machines up to 3 to 4 times.³⁹

In Pennsylvania, a poll worker observed a woman vote twice in the same day by changing her appearance.⁴⁰ Another poll worker observed people in voting lines in one corner of a polling location voting, and then coming to another polling location at the other side of the building to vote.⁴¹ Still another poll worker witnessed a woman voting twice at voting machines on Election Day.⁴²

IV. Ballot Mishandling

Ballot mishandling represents the second major dimension of alleged election irregularities in the 2020 presidential election. As Table 4 illustrates, this is a multifaceted problem across the battleground states. Let's work our way through this figure starting with the failure to properly check the identification of voters.

ARIZONA GEORGIA MICHIGAN NEVADA PENNSYLVANIA WISCONSIN No Voter I.D. Check Signature Match Check Abuses "Naked Ballots" Lacking **Outer Envelope** Broken Chain of Custody & **Unauthorized Ballot Handling or Movements Ballots Accepted Without** Postmarks & Backdating of Ballots = Wide-Spread Evidence * = Some Evidence

Table 4: Ballot Mishandling in the Battleground States

No Voter I.D. Check

It is critical for the integrity of any election for poll workers to properly verify a voter's identity and registration when that voter comes in to cast an in-person ballot. However, there is at least some evidence of a lack of adequate voter ID check across several of the battleground states.

For example, in Michigan, the chairperson of a polling location permitted an individual to vote without presenting voter identification and another with only a photocopy of a driver's license. 43

In Nevada, poll workers were instructed to advise people who wanted to register to vote and did not have proper Nevada IDs or Driver's Licenses to do the following: These unregistered voters could go outside into the parking lot and make an appointment with the Department of Motor Vehicles as late as January 2021 to obtain a Nevada Driver's License as proof of their identity. They could then bring in confirmation of their DMV appointment in either paper or digital form; and that would be sufficient to allow them to be registered.⁴⁴

Signature Matching Abuses

It is equally critical that ballot counters legally verify mail-in and absentee ballots by checking if the signatures on the outer envelopes match the voters' registration records.⁴⁵ Note, however, that a variety of signature matching abuses represent a major issue in Nevada, Pennsylvania, and especially in Georgia.

In Georgia, contrary to state law, the Secretary of State entered into a Consent Decree with the Democrat Party that weakened signature matching to just one verification instead of two. This illegal weakening of the signature match test has called into question more than 1.2 million mailin ballots cast in Georgia.⁴⁶

Georgia is not the only state where signature match check abuses have surfaced. Nevada law requires that *persons* – not machines – review all signatures and ballots. Yet the Clark County Registrar of Voters used a defective signature matching computer system called Agilis to conduct such checks. As will be discussed further below, this problem of machines replacing humans contrary to Nevada state law was compounded by the fact that the Agilis system has an unacceptably low accuracy rate, making it easier for illegal ballots to slip through its screen. As

Signature match abuses also surfaced in Wisconsin where mandatory voter information certifications for mail-in ballots were reduced and/or eliminated, again contrary to state law. As noted in one lawsuit, this change "undermined the authority of the state legislature, reduced the security and integrity of the election by making it easier to engage in mail-in ballot fraud and created another standard-less rule in conflict with the clear terms of the Wisconsin Election Code, preventing uniform treatment of absentee ballots throughout the State."

"Naked Ballots" Lacking Outer Envelope

A *naked ballot* is a mail-in or absentee ballot lacking an outer envelope with the voter's signature on it. It is illegal to accept the naked ballot as the outer envelope provides the only way to verify a voter's identity.

The illegal acceptance of naked ballots appears to be particularly acute in Pennsylvania as a result of ill-advised "guidance" issued by the Secretary of State – a registered Democrat⁵⁰ – that such naked ballots be counted.

This issuance of such guidance, in violation of state law,⁵¹ appears to be a blatant attempt by a Democrat politician to boost the count for Joe Biden as it was clear that Democrats would be voting disproportionately higher through mail-in ballots. This incident is especially egregious because when the Pennsylvania Supreme Court rejected this guidance, the Secretary of State refused to issue new guidance directing election officials to NOT count non-compliant mail-in or absentee ballots.⁵²

Broken Chain of Custody & Unauthorized Ballot Handling or Movements

The maintenance of a proper chain of custody for ballots cast is the linchpin of fair elections. Chain of custody is broken when a ballot is fraudulently transferred, controlled, or moved without adequate supervision or oversight.⁵³

While chain of custody issues can apply to all ballots, the risk of a broken chain of custody is obviously higher for mail-in and absentee ballots. This is because the ballots have to go through more hands.

In the 2020 presidential election, the increased use – often illegal use – of unsupervised drop boxes arguably has enhanced the risk of a broken chain of custody. So, too, has the increased practice of so-called "ballot harvesting" whereby third parties pick up ballots from voters and deliver them to drop boxes or directly to election officials.

Both drop boxes and ballot harvesting provide opportunities for bad actors to insert fraudulent ballots into the election process. That this is a very serious matter is evident in this observation by BlackBoxVoting.org: "In court cases, chain of custody violations can result in refusal to admit evidence or even throwing a case out. In elections, chain of custody violations can result in 'incurable uncertainty' and court orders to redo elections." ⁵⁴ (emphasis added)

As an example of the drop box problem, in Pennsylvania, ballots were illegally dumped into drop boxes at the Nazareth ballot drop center in violation of state law.⁵⁵ Likewise in Pennsylvania, a man caught on videotape and photos came out of an unmarked Jeep extracting ballots from an unsupervised ballot drop-box to bring them into a ballot counting center. That same man was observed to come back with an empty ballot container to place in the unsupervised drop box.⁵⁶

In Wisconsin, the state's Election Committee illegally positioned <u>five hundred</u> drop boxes for collection of absentee ballots across the state. However, these drop boxes were disproportionately located in urban areas which tend to have much higher Democrat registration, thereby favoring the candidacy of Joe Biden. Note: <u>Any</u> use of a drop box in Wisconsin is illegal by statute. Therefore, the votes cast through them cannot be legally counted in any certified election result.⁵⁷

As an example of ballot harvesting – in this case at the front end of the process – 25,000 ballots were requested from nursing home residents in Pennsylvania at the same time.⁵⁸

As additional examples of a possible broken chain of custody, there are these: Large bins of absentee ballots arrived at the Central Counting Location in Wisconsin with already opened envelopes, meaning that ballots could have been tampered with.⁵⁹ They were nonetheless counted.

Also in Wisconsin, an election worker was observed moving bags of blank ballots into a vehicle and then driving off without supervision.⁶⁰ There is also the previously referenced case whereby a truck driver has offered a firsthand account of moving large quantities of fake manufactured ballots from New York to Pennsylvania.

As a final note on the unauthorized handling or movement of ballots, there is the problem of *illegal* ballot counters. These are persons who not legally permitted and/or certified to be counting ballots.

In one curious case, an individual who worked as an official photographer for Kamala Harris' campaign in 2019⁶¹ was alleged to be involved in scanning ballots in Floyd County, Georgia. Ballot counters cannot have any ties to candidates in a presidential election.

Ballots Accepted Without Postmarks and Backdating of Ballots

Across all of the battleground states, it is against state law for poll workers to count either mail-in or absentee ballots that lack postmarks. It is also illegal to backdate ballots so that they may be considered as having met the election deadline for the receipt and counting of such ballots. There is some evidence of these irregularities in several of the battleground states.

For example, in Wisconsin, according to one Declaration, employees of the United States Postal Service (USPS) in Milwaukee were repeatedly instructed by two managers to backdate latearriving ballots so they could still be counted. ⁶² In addition, the USPS was alleged to have backdated as many as 100,000 ballots in Wisconsin. ⁶³

Similarly, in Detroit, Michigan, as noted in a court case, poll workers were instructing ballot counters to backdate absentee ballots so they could be counted.⁶⁴ One poll watcher also observed ballots in Michigan being run through vote tabulation machines without postmarks on them.⁶⁵

V. Contestable Process Fouls

Contestable process fouls represent the third dimension of election irregularities in the 2020 presidential election. The various forms such process fouls can take are illustrated in Table 5 across the six battleground states.

PENNSYLVANIA WISCONSIN ARIZONA GEORGIA MICHIGAN NEVADA Abuses of Poll Watchers & **Observers** Mail-In & Absentee Ballot Rules Violated Contrary to State Law Voters Not Properly Registered Allowed to Vote Illegal Campaigning at Poll Locations **Ballots Cured by Poll Workers** or Voters Contrary to Law = Wide-Spread Evidence * = Some Evidence

Table 5: Contestable Process Fouls in the Battleground States

Abuses of Poll Watchers and Observers

Central to the fairness and integrity of any election is the processes by which observers monitor the receipt, opening, and counting of the ballots. You can see in the Table 5 that poll watcher and observer abuses were present across all six battleground states.

In Georgia,⁶⁶ Michigan,⁶⁷ and Pennsylvania,⁶⁸ poll watchers and observers were denied entry to ballot counting centers by Judges of Elections and other poll workers. This was despite presenting proper certification and identification.

In Georgia,⁶⁹ Michigan,⁷⁰ Nevada,⁷¹ and Pennsylvania,⁷² Republican poll watchers were also forced inside confined areas, thereby limiting their view. In some cases, this confinement was enforced by local law enforcement.

Across these four battleground states, Republican poll watchers were also directed to stand at unreasonably lengthy distances from ballot counters. In Michigan – arguably the "first among equals" when it comes to observer abuses – poll workers put up poster boards on the windows of the room where ballots were being processed and counted so as to block the view.⁷³ In Pennsylvania, tens of thousands of ballots were processed in back rooms where poll observers were prohibited from being able to observe at all.⁷⁴

This is an extremely serious matter because it is these poll watchers and observers who represent the frontline defenders of a fair election process. Their job is to make sure all ballots are handled properly and tabulated accordingly. They seek to answer questions like: Is there a signature match process being conducted? Does each ballot have an outer envelope or is it a naked ballot? Are ballots being run more than once through the tabulation machines?

When poll watchers or observers are barred from viewing or forced to view from unacceptably large distances, these watchdogs cannot accurately answer these questions. They, therefore, cannot fulfill their critical watchdog function.

Mail-In Ballot and Absentee Ballot Rules Violated Contrary to State Law

In Georgia, more than 300,000 individuals were permitted to vote who had applied for an absentee ballot more than 180 days prior to the Election Day. This is a clear violation of state law.⁷⁵

In both Pennsylvania and Wisconsin, Democrat election officials acted unilaterally to accept both mail-in and absentee ballots after Election Day. State Republicans have argued this is contrary to state law.

In Pennsylvania, absentee and mail-in ballots were accepted up to three days after Election Day.⁷⁶ On November 7th, in anticipation of a legal challenge, the United States Supreme Court ordered that the approximately 10,000 absentee and mail-in ballots that had arrived past November 3rd be separated from ballots that had arrived on Election Day.⁷⁷ This direction notwithstanding, a poll watcher reported on November 7th that, in Delaware County, ballots received the previous night were not being separated from ballots received on Election Day, contrary to state law.⁷⁸

Wisconsin state law does not permit early voting. Nonetheless, city officials in the Democrat stronghold of Madison, Wisconsin assisted in the creation of more than 200 "Democracy in the Park" illegal polling places.

These faux polling places were promoted and supported by the Biden campaign. They provided witnesses for absentee ballots and acted in every way like legal polling places. Moreover, they received ballots outside of the limited 14-day period preceding an election that is authorized by statute for in-person or absentee balloting. These were clear violations of state law.⁷⁹

Voters Not Properly Registered Allowed to Vote

One of the jobs of poll workers is to ensure that in-person voters are legally registered and are who they say they are. Across at least three of the six battleground states – Georgia, Nevada, and Wisconsin – this job may not have been effectively done.

In Wisconsin, for example, officials refused to allow poll watchers to challenge the qualifications of people applying to vote or require proof of such persons' qualifications. ⁸⁰ In Georgia, more than 2,000 individuals appear to have voted who were not listed in the State's records as having been registered to vote. ⁸¹

In Pennsylvania, a poll watcher observed poll workers taking individuals whose names did not appear in voter registration books back into a separate area that was unobserved by any poll watchers. There, these apparently unregistered voters met with a Judge of Elections who allegedly told them: "you go back in, tell them this is your name, and you can vote." 82

Illegal Campaigning at Poll Locations

Poll workers are supposed to remain politically neutral. When a poll worker displays bias for one political candidate over another at a polling location, this is contrary to state law. Unfortunately, this law appears to have been repeatedly violated in Michigan, Pennsylvania, and Wisconsin.

For example, in Pennsylvania, poll workers were wearing paraphernalia from a group called "Voter Protection." This is a 100% Democrat-funded Political Action Committee dedicated to Democrat redistricting in Pennsylvania; and the wearing of its paraphernalia constitutes illegal campaigning at the polls.⁸³

In a similar type of illegal campaigning in Michigan, poll workers were allowed to wear Black Lives Matter shirts and were seen carrying tote bags of President Obama paraphernalia.⁸⁴ In addition, poll workers with Biden and Obama campaign shirts on were allowed on the ballot counting floor.⁸⁵

In Wisconsin, representatives from the Biden campaign were outside with clipboards talking to voters on their way in to vote. They were clearly inside the prohibited perimeter for electioneering. Poll workers did nothing to address this illegal campaigning despite the objections of observers.⁸⁶

Ballots Cured by Poll Workers or Voters Contrary to Law

Under prescribed circumstances, both poll workers and voters may fix ballots with mistakes or discrepancies. This process is known as "ballot curing."

In nineteen states, poll workers must notify voters if there are errors or discrepancies on their ballots and allow them to "cure" or correct any errors so their votes will count. Representates that do not allow curing, ballots with discrepancies such as missing or mismatched signatures must be discarded. Representation of the states are errors or discrepancies on their votes will count. The states that do not allow curing, ballots with discrepancies such as missing or mismatched signatures must be discarded.

In Pennsylvania, and contrary to state law, poll workers were trained to allow voters to cure or "correct" their ballots. ⁸⁹ According to one court filing, Democrat-controlled counties in Pennsylvania participated in pre-canvass activities prior to Election Day "by reviewing received mail-in ballots for deficiencies." ⁹⁰ Such discrepancies included "lacking the inner secrecy envelope or lacking a signature of the elector on the outer declaration envelope." Voters were then notified so that they could cure their ballots – a clear violation of state law. ⁹¹

Numerous other examples of illegally cured ballots abound. For example, in Wisconsin, tens of thousands of ballots were observed to be corrected or cured despite election observer objections. 92

In Pennsylvania, poll workers sorted approximately 4,500 ballots with various errors into bins. Poll workers then re-filled out the 4,500 ballots so that they could be read by tabulation machines, an action contrary to state law.⁹³

In Michigan, poll workers altered the dates on the outer envelopes of the ballots so that they would be able to count them.⁹⁴ Michigan poll workers also filled out blank ballots to "correct" mail-in and absentee ballots according to what they believed the "voter had intended."⁹⁵

VI. Equal Protection Clause Violations

The Equal Protection Clause is part of the 14th Amendment of the U.S. Constitution and a fundamental pillar of the American Republic. This Equal Protection Clause mandates that no State may deny its citizens equal protection of its governing laws. ⁹⁶

Table 6 illustrates three major alleged violations of the Equal Protection Clause in the 2020 presidential election. As the table illustrates, each violation was observed to occur across all six battleground states.

ARIZONA GEORGIA MICHIGAN NEVADA PENNSYLVANIA WISCONSIN

Higher Standards of
Certification & I.D.
Verification Applied to InPerson Voters

Different Standards of
Ballot Curing

Differential & Partisan
Poll Watcher Treatment

V = Wide-Spread Evidence *= Some Evidence

Table 6: Equal Protection Clause Violations in the Six Battleground States

Higher Standards of Certification & I.D. Verification Applied to In-Person Voters

The first alleged violation focuses on the application of higher standards of certification and voter identification for in-person voters than mail-in and absentee ballot voters. In effect, these higher standards disproportionately benefited the candidacy of Joe Biden because President Trump had a much higher percentage of in-person voters than mail-in and absentee voters. Indeed, mail-in and absentee ballots were largely skewed for Joe Biden across the country by ratios as high as 3 out of 4 votes in some states.⁹⁷

Note here that much of the alleged fraud and ballot mishandling focused on mail-in voters and absentee ballots. Therefore, the lower the level of scrutiny of these voters, the more illegal votes for Joe Biden relative to Donald Trump could slip in. It should likewise be noted here that this particular violation of the Equal Protection Clause was further enabled by poll watchers being denied meaningful observation.

Perhaps the most egregious examples of this particular violation of the Equal Protection clause occurred in Georgia and Michigan. Georgia, for example, requires ID for voting in-person and Michigan will only allow provisional voting without an ID. However, in both Georgia and Michigan, a valid ID is not required to vote by mail so long as the person has already registered in a previous election.

These procedures are ripe for fraud. In fact, there is evidence that election fraudsters targeted voters who had voted in past elections but not voted in more recent ones. These fraudsters could then cast ballots on behalf of these infrequent voters with little likelihood they would be caught. Numerous affidavits, however, detail persons arriving to vote at polls only to be informed that records indicate they had already voted. At least fourteen such affidavits have been made by Georgians.

As a further example, in Wisconsin, mail-in ballots were accepted without witness signatures placed properly in the allocated envelope location.⁹⁸ A comparable process for in-person voting would have resulted in the invalidation of the vote.

Different Standards of Ballot Curing

As a second major violation of the Equal Protection Clause, likewise observed across all six battleground states, different standards for correcting mistakes on ballots (ballot curing) were applied across different jurisdictions within the states. Often, jurisdictions with predominantly Democrat registration were more expansive about allowing the curing of ballots than jurisdictions with predominantly Republican registration.

In Pennsylvania, there was a clear difference between how ballots were – or were not – cured in Republican counties versus Democrat counties. When Pennsylvania's Secretary of State Kathy Boockvar issued illegal guidance authorizing counties to cure ballots, this illegal guidance was not followed in at least eight different Republican counties. Meanwhile, ballots were cured in Democrat counties under this illegal guidance.

In Arizona, there likewise was a clear difference between how in-person voters were treated versus mail-in ballots. On the one hand, mail-in voters had up to 5 days to "cure" or "fix" invalid mail-in ballots sent prior to Election Day.¹⁰¹ On the other hand, in-person voters in Maricopa County, for example, had to deal with poll workers who did not know how to work electronic voting machines properly. This resulted in thousands of in-person votes being marked incorrectly and disregarded rather than cured.¹⁰²

Differential and Partisan Poll Watcher Treatment

In most states, political party candidates and ballot issue committees are able to appoint poll watchers and observers to oversee the ballot counting process. ¹⁰³ Such poll watchers and observers must be registered voters and present certification to the Judge of Elections in order to be able to fulfill their duties at a polling location. ¹⁰⁴

Such certified poll watchers should be free to observe at appropriate distances regardless of their party affiliation. Yet in key Democrat strongholds, e.g., Dane County in Wisconsin and Wayne County in Michigan, which yielded high Biden vote counts, Republican poll watchers and observers were frequently subject to different treatment ranging from denial of entry to polling places to harassment and intimidation.

For example, in Georgia, a certified poll watcher witnessed other poll workers at a polling location discussing how they should not speak to her due to her party affiliation. ¹⁰⁵ In Pennsylvania, a Republican poll watcher was harassed and removed from the polling location due to his party affiliation. ¹⁰⁶ In Wisconsin, a Republican poll watcher was prevented from observing due to the fact that polling locations were not allowing Republicans in. ¹⁰⁷

Note the synergy here between the problem of the process foul involved with denying access to certified poll watchers (discussed in the previous section) and the violation of the Equal Protection Clause such conduct entails when such denial, harassment, and intimidation differs by party affiliation.

VII. 2020 Election Voting Machine Irregularities

Perhaps no device illustrates that technology is a double-edged sword than the machines and associated software that have come to be used to tabulate votes across all 50 states. ¹⁰⁸ Types of voting equipment include optical scanners used to process paper ballots, direct recording electronic systems which voters can use to directly input their choices, and various marking devices to produce human-readable ballots. ¹⁰⁹

Two main types of voting machine irregularities have been alleged in the 2020 presidential election. As Table 7 illustrates, these types of irregularities include large-scale voting machine inaccuracies together with inexplicable vote switching and vote surges, often in favor Joe Biden.



Table 7: 2020 Voting Machine Irregularities

Large-Scale Voting Machine Inaccuracies

Much has been made about the shadowy genesis of a company called Dominion which provides voting machines and equipment to 28 states. According to critics, Dominion's roots may be traced to an effort by the Venezuelan dictator Hugo Chavez to rig his sham elections. Dominion is also alleged to have ties to the Clinton Foundation, while the Smartmatic software used in the Dominion machines is alleged to have links to the shadowy anti-Trump globalist financier George Soros. 113

The controversy swirling over Dominion and Smartmatic notwithstanding, one of the biggest problems with machine inaccuracies may be traced to a company called Agilis. Nevada election officials in Clark County, a Democrat stronghold in Nevada, used Agilis signature verification machines to check over 130,000 mail-in ballot signatures.

According to a court case filed in the First Judicial District Court in Carson City, the Agilis machines used a "lower image quality than suggested by the manufacturer." Clark County Election Department officials also lowered the accuracy rate below the manufacturer's recommendations, making the whole verification process unreliable. 114

In a test run, it was proven that, at the manufacturer's setting, the Agilis machine already had a high tolerance for inaccuracies—as high as 50% non-matching. In other words, half of the ballots that might be moved through the machine would be impossible to verify; and Clark County officials lowered that threshold even further. 115

As a final comment on this case, there is also the broader legal matter that the Agilis machines were used to "entirely replace signature verification by election personnel." This is contrary to Nevada state law.

As noted in a court case: "In violation of Nevada law, the Clark County Election Department allows the Agilis machine to solely verify 30% of the signatures accompanying the mail-in ballots without ever having humans inspect those signatures." ¹¹⁶

A similar problem has been alleged in a court filing in Arizona with a software known as the Novus 6.0.0.0. In cases where ballots were too damaged or illegible to be read by vote tabulation machines, Novus was used in an attempt to cure or restore the ballots. The system would do so by trying to read the applicable scans of the original rejected ballots. However, as noted in a court case filed by Kelli Ward, Chairwoman of the Arizona Republican Party: "the software was highly inaccurate, and it often flipped the vote." 117

Inexplicable Vote Switching and Vote Surges In Favor of Biden

As a further complication to the Novus software problem in Arizona referenced above, the software was not only highly inaccurate. According to observers, and as an example of inexplicable vote switching, "the software would erroneously prefill 'Biden' twice as often as it did 'Trump." 118

At least one instance of a large and inexplicable vote switching and vote surge in favor of Joe Biden took place in Antrim County, Michigan – and it is associated with the controversial aforementioned Dominion-Smartmatic voting machine hardware-software combo. ¹¹⁹ In this Republican stronghold, 6,000 votes were initially, and incorrectly, counted for Joe Biden. The resulting vote totals were contrary to voter registration and historical patterns and therefore raised eyebrows. When a check was done, it was discovered that the 6,000 votes were actually for Donald J. Trump.

A subsequent forensic audit of the Antrim County vote tabulation found that the Dominion system had an astonishing error rate of 68 percent. By way of comparison, the Federal Election Committee requires that election systems must have an error rate no larger than 0.0008 percent. Plant 121

Perhaps even more troubling given concerns over hackers and Dominion's alleged ties to bad foreign actors, the records that would have allowed the detection of remote internet access went missing from the Antrim County system. This was in direct violation of Michigan state law, 122 which requires retention of voting records for 22 months -- such information was in place for previous election years, but not this election. At the very least, the results of this audit indicates the need for further investigation of the Dominion system across other states in the country.

In Georgia, there were numerous "glitches" with the Dominion machines where the results would change. The most notable of these changes was a 20,000 vote surge for Biden and 1,000 vote decrease for Trump. 123

VIII. Statistical Anomalies in the Six Battleground States

The 2020 presidential election appears to feature at least four types of statistical anomalies that raise troubling questions. Table 8 illustrates the incidence of these statistical anomalies across the six battleground states. As you can see from the table, Wisconsin and Georgia are characterized by the highest degree of statistical anomalies, with three of the four anomalies present. Nevada and Arizona show two anomalies present while Michigan has at least one. Let's take a more granular look now at each of these types of statistical anomalies.

GEORGIA PENNSYLVANIA WISCONSIN ARIZONA MICHIGAN NEVADA Significant Changes In Absentee Ballot Rejection **Rates From Previous Elections Excessively High Voter Turnout** (at times exceeding 100%) Statistically improbable Vote **Totals Based on Party** Registration & Historical **Patterns Unusual Vote Surges** = Wide-Spread Evidence = = Some Evidence

Table 8: Statistical Anomalies in the Battleground States

Dramatic Changes in Mail-in and Absentee Ballot Rejection Rates from Previous Elections

It is routine across the 50 states for mail-in-and absentee ballots to be rejected for any number of reasons. These reasons may include: the lack of a signature or adequate signature match, a late arrival past a deadline, ¹²⁴ the lack of an external envelope that verifies voter-identification (a naked ballot), ¹²⁵ or if voters provide inaccurate or incomplete information on the ballots. ¹²⁶

In the 2020 presidential race, Joe Biden received a disproportionately high percentage of the mailin and absentee ballots. Perhaps not coincidentally, we saw a dramatic fall in rejection rates in Pennsylvania, Nevada, and especially Georgia.

For example, in Nevada, the overall rejection rate dropped from $1.6\%^{127}$ in 2016 to 0.58% in 2020. The Pennsylvania, the 2016 rejection rate of $1.0\%^{129}$ dropped to virtually nothing at 0.28%. The biggest fall in the overall absentee ballot rejection rate came, however, in Georgia. Its rejection rate fell from $6.8\%^{131}$ in 2016 to a mere $0.34\%^{132}$ in 2020.

These dramatically lower rejection rates point to a conscious effort by Democrat election officials across these key battleground states to subject mail-in and absentee ballots to a lower level of scrutiny. That this kind of government conduct and gaming of our election system may have contributed to tipping the scales in favor of Joe Biden can be illustrated in this simple calculation:

In the 2020 race, Georgia election officials received 1,320,154 mail-in and absentee ballots. If these ballots had been rejected at the 2016 rate of 6.8% instead of the 2020 rate of 0.34%, there would have been 81,321 ballots rejected instead of the 4,489 ballots that were actually rejected.

Under the conservative assumption that 60% of these mail-in and absentee ballots went to Joe Biden, ¹³³ this dramatic fall in the rejection rate provided Joe Biden with an additional 16,264 votes. That's more than the margin of the alleged Biden victory in Georgia.

Excessively High Voter Turnout (at times exceeding 100%)

When there are more ballots cast than registered or eligible voters, fraud has likely taken place. During the 2020 presidential election, excessively high voter turnout occurred across all six swing states.

In analyzing this problem, it is important to distinguish between states that have same-day registration and those that don't. States with same-day registration can plausibly have voter turnout that is higher than 100%. However, is impossible for that to happen in states without same-day registration without fraud having taken place.

Consider, then, Arizona which does not allow same-day voter registration. According to testimony from an MIT-trained mathematician, Candidate Biden may have received a weighted 130% total of Democrat votes in Maricopa County to help him win the state due to an algorithm programmed into the Dominion voting machines used there. 134

Although Michigan does allow same-voter registration, voter turnout was still abnormally high. Here again, the Dominion voting system has been implicated. To wit:

Cybersecurity executive and former NASA analyst, Russ Ramsland, testified that in Wayne County, Michigan, where Dominion Voting Systems equipment was used, 46 out of 47 precincts in the county displayed greater than a 96% voter turnout. 25 out of those precincts showed a 100% voter turnout. 135

Wisconsin, which also allows same-day voter registration, also reported abnormally high voter turnout when compared to 2016 numbers. For example, Milwaukee reported a record 84% voter turnout during the 2020 presidential election versus 75% in 2016. ¹³⁶ Of the city's 327 voting wards, 90 reported a turnout of greater than 90%. ¹³⁷

Statistically Improbable Vote Totals Based on Party Registration and Historical Patterns

The 2020 presidential election was characterized by strong partisan voting patterns consistent with historical patterns. As a rule, heavily Republican jurisdictions voted heavily for President Trump and heavily Democrat jurisdictions voted heavily for Joe Biden.

In some cases, however, there were instances where these partisan and historical patterns were violated. It is precisely in such instances where either outright fraud or machine inaccuracies or manipulations are most likely to be operative.

As one example of such statistically improbable vote totals, there are the results in Arizona's Fifth Congressional District. In one precinct in the suburb of Queen Creek, the vote percent for President Trump dropped dramatically relative to 2016, from 67.4 to 58.5 percent. ¹³⁸ This was attributed to an "unusually high" number of duplicate ballots. ¹³⁹

Unusual Vote Surges

Several unusual vote surges took place in the very early hours of the morning of November 4th in Georgia, Michigan, and Wisconsin. An analysis conducted by the Voter Integrity Project of *The New York Times* publicly reported data on Election Day that showed several vote "spikes" that were unusually large in size with unusually high Biden-to-Trump ratios. Such spikes or surges could well indicate that fraudulent ballots had been counted.

IX. A State-By-State Analysis and Signal Failure of Our Legislative and Judicial Branches

All happy families are alike; each unhappy family is unhappy in its own way.

- Anna Karenina, by Leo Tolstoy

It should be clear at this point that all six battleground states suffer from most or all of the six dimensions of election irregularities documented in this report. However, like Tolstoy's unhappy families, it is also true that each battleground state is different in its own election irregularity way. That is, each battleground state may be characterized by a unique mix of issues that, impressionistically, might be considered "most important" in swinging that state for Joe Biden.

Consider Arizona, a state with the lowest alleged Biden victory margin at 10,457 votes. This is a state with statistically improbable high voter turnouts in Maricopa and Pima counties; widespread ballot mishandling; and 1.6 million mail-in ballots (which tended towards Biden) subjected to much lower standards of certification and ID verification than in-person voters (who tended towards Trump).

In Georgia, the alleged Biden victory margin was just 11,779 votes. What perhaps jumps out most in the Peach State is the illegal Consent Decree that effectively gutted the signature match requirements for millions of mail-in ballots. There is also the quite unresolved fake ballot manufacturing matter of the roughly 100,000 ballots that were mysteriously pulled, in the dead of night, out from underneath tables and expeditiously tabulated. Of course, we saw that Georgia's electoral version of a Three-card Monte sleight-of-hand led to a strong Biden vote surge.

Of all of the six battleground states which suffered from numerous observer and poll watcher abuses, Michigan must rank as "first among equals." With its "board up the windows" and "rough up the observers" tactics, Detroit in Wayne County was the center of this "see no evil" universe. When two local Republican officials tried to withhold certification of the votes in this county for practices such as these and demanded an audit, they were subject to extreme intimidation and "doxing" and quickly capitulated.¹⁴³

As for Nevada, this is a state likewise with a very narrow alleged victory margin for Joe Biden – 33,596 votes. Here, voting machine irregularities associated with the Agilis machine have called into question as many as 130,000 votes. There may also be an unusually large number of ballots cast by out-of-state voters and others who did not meet residency requirements. Of course, the brazen bribery of Native Americans to vote for Joe Biden is a dark stain on the state and the Democrat Party. ¹⁴⁴

In Pennsylvania, an equally brazen Democrat Secretary of State issued illegal guidance for the acceptance of naked ballots and ignored direction from the Pennsylvania Supreme Court to fix the matter. She allowed ballots to be illegally cured in contravention of state law and pushed the legal envelope for accepting ballots after Election Day.

In the Keystone State, and as with Georgia's Three-card Monte, shuffle fake ballots out from underneath a table scandal, there is also the equally unresolved matter of possible fake ballot manufacturing. Recall, here, the testimony of a truck driver who swears he picked up as many as 100,000 fake manufactured ballots in New York and delivered them to Pennsylvania. Both the tractor-trailer and the ballots involved remain unaccounted for – and what might have been in this tractor-trailer were enough ballots alone to swing the election to Joe Biden.

Finally, in Wisconsin, the mother of all contestable process fouls is arguably that of the roughly 170,000 mail-in ballots entering the tabulation process under the guise of absentee ballots in clear violation of state law. That's more than eight times the number of ballots of the alleged Biden victory margin of 20,682 votes.

In Wisconsin, there is likewise the large-scale abuse associated with an overly expansive definition of "indefinitely confined voters." Recall here that the increment of new indefinitely confined voters in the 2020 election in Wisconsin was more than five times the alleged Biden victory margin.

While Democrat Party government officials cheated and gamed the electoral process across all six battleground states, many Republican government officials – from governors and state legislators to judges – did little or nothing to stand in their way.

Consider that the Republican Party controls *both* chambers of the State Legislatures in five of the six battleground states – Arizona, Georgia, Michigan, Pennsylvania, and Wisconsin.¹⁴⁵ These State Legislatures clearly have both the power and the opportunity to investigate the six dimensions of election irregularities presented in this report. Yet, wilting under intense political pressure, these politicians have failed in their Constitutional duties and responsibilities to do so – and thereby failed both their states and this nation as well as their party.

The same can be said for the Republican governors in two of the six battleground states – Arizona and Georgia. Both Arizona's Doug Ducey and Georgia's Brian Kemp have cowered in their Governor's mansions and effectively sat on their hands while their states have wallowed in election irregularities.

The judicial branch of the American government should be the final backstop for the kind of issues examined in this report. Yet both our State courts and Federal courts, including the Supreme Court, have failed the American people in refusing to properly adjudicate the election irregularities that have come before them. Their failures likewise pose a great risk to the American Republic.

Concluding Observations

From the findings of this report, it is possible to infer what may well have been a coordinated strategy to effectively stack the election deck against the Trump-Pence ticket. Indeed, the patterns of election irregularities observed in this report are so consistent across the six battleground states that they suggest a coordinated strategy to, if not steal the election, then to strategically game the election process in such a way as to unfairly tilt the playing field in favor of the Biden-Harris ticket.

A major part of this "stuff the ballot box" strategy has been aptly summarized in a complaint filed before the US Supreme Court by the State of Texas:

Using the COVID-19 pandemic as a justification, [Democrat] government officials [in Georgia, Michigan, Pennsylvania, and Wisconsin] usurped their legislatures' authority and unconstitutionally revised their state's election statutes. They accomplished these statutory revisions through executive fiat or friendly lawsuits, thereby weakening ballot integrity. 146

According to the Texas complaint – which the Supreme Court sadly refused to hear – the goal of this strategy was to flood the battleground states "with millions of ballots to be sent through the mails, or placed in drop boxes, with little or no chain of custody." At the same time, Democrat government officials also sought to "weaken the strongest security measures protecting the integrity of the vote signature verification and witness requirements." ¹⁴⁷

The findings of the assessment conducted in this report are consistent with the Texas complaint. Key takeaways include:

- The weight of evidence and patterns of irregularities uncovered in this report are such that
 it is irresponsible for anyone especially the mainstream media to claim that there is "no
 evidence" of fraud or irregularities.
- The ballots that have come into question because of the identified election irregularities are more than sufficient to swing the outcome in favor of President Trump should even a relatively small portion of these ballots be ruled illegal.
- While all six battleground states exhibit most, or all, six dimensions of election irregularities, each state has a unique mix of issues that might be considered "most important." To put this another way, all battleground states are characterized by the same or similar election irregularities; but, like Tolstoy's unhappy families, each battleground state is different in its own election irregularity way.
- This was theft by a thousand cuts across six dimensions and six battleground states rather than any one single "silver bullet" election irregularity.

- In refusing to investigate a growing number of legitimate grievances, the anti-Trump media and censoring social media are complicit in shielding the American public from the truth. This is a dangerous game that simultaneously undermines the credibility of the media and the stability of our political system and Republic.
- Those journalists, pundits, and political leaders now participating in what has become a Biden Whitewash should acknowledge the six dimensions of election irregularities and conduct the appropriate investigations to determine the truth about the 2020 election. If this is not done before Inauguration Day, we risk putting into power an illegitimate and illegal president lacking the support of a large segment of the American people.
- The failure to aggressively and fully investigate the six dimensions of election irregularities
 assessed in this report is a signal failure not just of our anti-Trump mainstream media and
 censoring social media but also of both our legislative and judicial branches.
 - Republican governors in Arizona and Georgia together with Republican majorities in both chambers of the State Legislatures of five of the six battleground states Arizona, Georgia, Michigan, Pennsylvania, and Wisconsin¹⁴⁸ have had both the power and the opportunity to investigate the six dimensions of election irregularities presented in this report. Yet, wilting under intense political pressure, these politicians have failed in their Constitutional duties and responsibilities to do so and thereby failed both their states and this nation as well as their party.
 - o Both State courts and Federal courts, including the Supreme Court, have failed the American people in refusing to appropriately adjudicate the election irregularities that have come before them. Their failures pose a great risk to the American Republic.
- If these election irregularities are not fully investigated prior to Inauguration Day and thereby effectively allowed to stand, this nation runs the very real risk of never being able to have a fair presidential election again with the down-ballot Senate races scheduled for January 5 in Georgia an initial test case of this looming risk.

ENDNOTES

¹ All witnesses who have signed sworn affidavits or declarations who are referenced in this report but whose names are not referenced in the public record, e.g., a court case, are referred to as "Jane Doe" or "John Doe" based on gender. This has been done to ensure their safety and security.

² Ballotopedia, "Partisan composition of state legislatures," December 4, 2020. https://ballotpedia.org/Partisan composition of state legislatures

³ Bump, Philip. "The two states that almost always predict which candidate is headed for defeat," *The Washington Post*, 7 September 2016. https://www.washingtonpost.com/news/the-fix/wp/2016/09/07/the-two-states-that-almost-always-predict-which-candidate-is-headed-for-defeat/

*The two Democrat candidate exceptions were John F. Kennedy in 1960 and Bill Clinton in 1992.

⁴ Williams, Pete. "Trump's election fight includes over 50 lawsuits. It's not going well." *NBC News*, November 23, 2020. https://www.nbcnews.com/politics/2020-election/trump-s-election-fight-includes-over-30-lawsuits-it-s-n1248289

⁵ All witnesses who have signed sworn affidavits and declarations referenced in this report are referred to as "Jane Doe" and "John Doe" based on gender, in order to ensure their safety and security.

⁶ Bannon, Steve, War Room Pandemic, https://pandemic.warroom.org/

⁷ Solomon, John, Just the News, https://justthenews.com/john-solomon

8 Kassam, Raheem, National Pulse, https://americasvoice.news/the-national-pulse/

9 Newsmax, https://www.newsmax.com/

10 One America News Network, https://www.oann.com/

11"Most Say Mail-In Voting Worked, But 47% Say Fraud Likely." Rasmussen Reports, December 7, 2020. https://www.rasmussenreports.com/public content/politics/elections/election 2020/most say mail in voting worked but 47 say fraud likely

¹² Legal Information Institute, "Bribery," Cornell University, https://www.law.cornell.edu/wex/bribery

¹³ Bedard, Paul, "Pro-Biden effort offered Native Americans \$25-\$500 Visa gift cards and jewelry to vote," Washington Examiner, December 14, 2020. https://www.washington-secrets/pro-biden-effort-offered-native-americans-25-500-visa-gift-cards-jewelry-to-vote

¹⁴ Pentochoukov, Ivan, "Illegal Money-for-Votes Raffles Conducted in Several States in 2020 Election," *Epoch Times*, December 2, 2020. https://www.theepochtimes.com/illegal-money-for-votes-raffles-conducted-in-several-states-in-2020-election 3598915.html

¹⁵ Morgan, Jessy. Testimony. "A truck driver with USPS says he was suspicious of his cargo load of 288,000 completed ballots." December 1, 2020. https://www.youtube.com/watch?v=R0xaA4dYsbQ

¹⁶ Declaration of John Doe, Delaware County Pennsylvania, November 9, 2020.

¹⁷ Bedard, Paul, "20 House Republicans demand Barr investigate 'suitcases' of ballots in Georgia," *The Washington Examiner*, December 4, 2020. https://www.washingtonexaminer.com/washington-secrets/20-house-gop-demand-agbarr-investigate-suitcases-of-ballots-in-georgia

¹⁸ "Trump Campaign lawyers present video 'evidence' of ballot fraud," Senate Judiciary Subcommittee, December 4, 2020. https://www.voutube.com/watch?v=LJ0xDWhWUxk

Real American Politics, December 4, 2020. https://twitter.com/RealAPolitics/status/1334754269052997635?s=20

¹⁹See, for example: Weber, Peter, "Georgia's top election investigator debunks a vote fraud conspiracy involving 'suitcases' of ballots, a urinal," December 7, 2020. https://news.yahoo.com/georgias-top-election-investigator-debunks-115236191.html

²⁰ In the United States District Court for the District of Arizona, *Tyler Bowyer et al v.. Doug Ducey*, December 2, 2020. https://www.democracydocket.com/wp-content/uploads/sites/45/2020/12/Bower-Complaint-AZ.pdf

²¹ Affidavit of Jane Doe, Cobb County, Georgia, November 12, 2020.

²² Declaration of Jane Doe, Bucks County, Pennsylvania, Nov 7, 2020

WisGOP, "WisGOP: Trump lawsuit highlights indefinitely confined voter increase," https://www.wispolitics.com/2020/wisgop-trump-lawsuit-highlights-indefinitely-confined-voter-increase/

WisGOP, "WisGOP: Some indefinitely confined voters are not indefinitely confined," https://www.wispolitics.com/2020/wisgop-some-indefinitely-confined/

²⁵ WisGOP, "WisGOP: Some indefinitely confined voters are not indefinitely confined," https://www.wispolitics.com/2020/wisgop-some-indefinitely-confined-voters-are-not-indefinitely-confined/

WisGOP, "WisGOP: Trump lawsuit highlights indefinitely confined voter increase," https://www.wispolitics.com/2020/wisgop-trump-lawsuit-highlights-indefinitely-confined-voter-increase/ Information Institute, "18 U.S. Code § 611. Voting aliens," Legal https://www.law.cornell.edu/uscode/text/18/611 The Superior Court Of Fulton County State Of Georgia, Trump v. Raffensperger, December 4, 2020. https://www.democracydocket.com/wp-content/uploads/sites/45/2020/12/Trump-v.-Raffensperger.pdf ²⁹ In the Superior Court of Fulton County State of Georgia, November 30, https://www.democracydocket.com/wp-content/uploads/sites/45/2020/11/2020-11-30-Verified-Complaint.pdf ³⁰ Declaration of Jane Doe, Philadelphia County, Pennsylvania, November 8, 2020. ³¹ In the First Judicial District Court Carson City, Nevada Jesse Law v. Judith Whitmer, November 17, 2020. https://www.democracydocket.com/wp-content/uploads/sites/45/2020/11/nov-17-doc-2.pdf ³² Declaration of John Doe, Las Vegas, Nevada, November 22, 2020. "Rudy Giuliani claims 8,000 dead people voted in election in Pennsylvania," November 25, 2020. https://www.youtube.com/watch?v=2 VUkB2jAcg See Also "Pennsylvania Senate Republican Lawmaker Hearing Transcript on 2020 Election," Rev., November 26, 2020. https://www.rev.com/blog/transcripts/pennsylvania-senate-republican-lawmaker-hearing-transcript-on-2020-election ³⁴ Affidavit of Jane Doe, Oakland County, Michigan, November 11, 2020. ³⁵ Declaration of John Doe, Clark County, Nevada, November 7, 2020. ³⁶ In the Superior Court of Fulton County State of Georgia, Paul Andrew Boland v Brad Raffensperger, November 2020. https://www.democracydocket.com/wp-content/uploads/sites/45/2020/11/2020-11-30-Verified-29, Complaint.pdf ³⁷ Statement of John Doe, Las Vegas, Nevada, November 20, 2020. ³⁸ Declaration of Jane Doe, Wisconsin, November 12, 2020. ³⁹ Affidavit of Jane Doe, Washtenaw County, Michigan, November 9, 2020. ⁴⁰ Declaration of Jane Doe, Northampton County, November 8, 2020. ⁴¹ Declaration of John Doe, Philadelphia County, November 14, 2020. ⁴² Declaration of Jane Doe, Northhampton County, Pennsylvania, November 7, 2020. ⁴³ Affidavit of John Doe, Michigan, November 10, 2020. ⁴⁴ Declaration of Jane Doe, Clark County, November 8, 2020. Ballotopedia, "How do election workers match signatures? (2020)," https://ballotpedia.org/How do election workers match signatures%3F (2020) ⁴⁶Democratic Party of Georgia, Inc. ("DPG"), the DSCC, and the DCCC, Compromise Settlement and Release, March 6, 2020. https://www.democracydocket.com/wp-content/uploads/sites/45/2020/07/GA-Settlement-L.pdf ⁴⁷Petition for Writ of Madamus and Complaint for Declaratory and Injunctive Relief, "Daniel Rodimer v. Joseph Gloria, November 19, 2020. https://www.democracydocket.com/wp-content/uploads/sites/45/2020/11/Rodimer-v-Gloria A-20-825130-W Writ-of-Mandamus.pdf ⁴⁸ In the First Judicial District Court Carson City, Nevada Jesse Law v. Judith Whitmer, November 17, 2020. https://www.democracydocket.com/wp-content/uploads/sites/45/2020/11/nov-17-doc-2.pdf ⁴⁹ In the United States District Court Eastern District of Wisconsin Milwaukee Division, Donald J. Trump v. the https://www.democracydocket.com/wp-Wisconsin Elections Commission. December 2020. content/uploads/sites/45/2020/12/Trump-v-WEC-EDW1.pdf 50 Ballotopedia, "Pennsylvania Secretary of State," https://ballotpedia.org/Pennsylvania Secretary of State ⁵¹ The United States District Court for the Middle District of Pennsylvania, Donald J. Trump for President et al v. Boockvar November, Kathy et al, https://www.courtlistener.com/recap/gov.uscourts.pamd.127057/gov.uscourts.pamd.127057,169.0.pdf 52 The United States District Court for the Middle District of Pennsylvania, Donald J. Trump for President et al v. November, 2020. et Kathy Boockvar al. https://www.courtlistener.com/recap/gov.uscourts.pamd.127057/gov.uscourts.pamd.127057.169.0.pdf Building," The Elections Assistance Commission. "Ballot https://www.eac.gov/sites/default/files/eac_assets/1/6/Chapter_5_Ballot_Building.pdf 54 Harris, Bev, "About Chain of Custody," Election Watch, February 16, 2016. https://blackboxvoting.org/about-

chain-of-custody/

⁵⁵ Declaration of Jane Doe, Pennsylvania, November 7, 2020. Northhampton County.

⁵⁶ Declaration of John Doe, Delaware County, Pennsylvania, November 7, 2020. (3 Pictures, 2 Videos)

- 57 In the Supreme Court of the United States, The State of Texas v. Commonwealth of Pennsylvania, State of Georgia, State of Michigan, State of Wisconsin, December 7, 2020. https://www.texasattorneygeneral.gov/sites/default/files/images/admin/2020/Press/SCOTUSFiling.pdf
- ⁵⁸ Chaitin, Daniel, "Lindsey Graham: Possible ballot harvesting in Pennsylvania involving 25,000 nursing home residents," *Microsoft News*, November 10, 2020. https://www.msn.com/en-us/news/politics/lindsey-graham-possible-ballot-harvesting-in-pennsylvania-involving-25-000-nursing-home-residents/ar-BB1aR3R4
- ⁵⁹ Affidavit of Jane Doe, Brookfield, Wisconsin, November 10, 2020.
- ⁶⁰ Declaration of John Doe, Brown County, November 11, 2020.
- ⁶¹ Greenberg, Jay, "Dominion Technician Exposed as Anti-Trump Ex-Kamala Harris Worker," December 1, 2020. https://neonnettle.com/news/13425-dominion-technician-exposed-as-anti-trump-ex-kamala-harris-worker
- 62 Declaration of Jane Doe, Waukesha County, Wisconsin, November 11, 2020.
- 63 " 'USPS contractor: "Something profoundly wrong occurred in Wisconsin during the presidential election' "
 December 1, 2020. https://www.youtube.com/watch?v=hRUvP6cbtZk&feature=youtu.be&t=69
 See also
- Van Brugen, Isabel, "Wisconsin USPS Subcontractor Alleges Backdating of Tens of Thousands of Mail-In Ballots," December 2, 2020. https://www.theepochtimes.com/wisconsin-usps-subcontractor-alleges-backdating-of-tens-of-thousands-of-mail-in-ballots 3601580.html
- ⁶⁴ State of Michigan Judicial District, Cheryl A. Constantino and David A. Kallman v. City of Detroit, November 8, 2020. https://assets.documentcloud.org/documents/20403147/wayne-county-michigan-election-fraud-lawsuit.pdf
- 65 Affidavit of Jane Doe, Oakland County, Michigan November 10, 2020.
- ⁶⁶ Declaration of John Doe, Cobb County, Georgia, November 5, 2020.
- ⁶⁷ Affidavit John Doe, Eagle County, Colorado November 12, 2020.
- ⁶⁸ The Declaration of John McBlain, Esquire. See, The Supreme Court of the United States, State of Texas v. Commonwealth of Pennsylvania, State of Georgia, State of Michigan, and State of Wisconsin, December 7, 2020. https://www.supremecourt.gov/DocketPDF/22/220155/163048/20201208132827887 TX-v-State-ExpedMot%202020-12-07%20FINAL.pdf
- ⁶⁹ Affidavit of Jane Doe, Gwinnett County, Georgia, November 12, 2020.
- ⁷⁰ Affidavit John Doe, Waukesha County, Wisconsin, November 10, 2020.
- ⁷¹ Affidavit of Jane Doe, Clark County, Nevada, November 10, 2020.
- ⁷²The Declaration of John McBlain, Esquire. See, The Supreme Court of the United States, State of Texas v. Commonwealth of Pennsylvania, State of Georgia, State of Michigan, and State of Wisconsin, December 7, 2020. https://www.supremecourt.gov/DocketPDF/22/220155/163048/20201208132827887 TX-v-State-ExpedMot%202020-12-07%20FINAL.pdf
- ⁷³ Affidavit of John Doe, November 10, 2020, Waukesha County, Wisconsin.
- ⁷⁴ The Declaration of John McBlain, Esquire. See, The Supreme Court of the United States, State of Texas v. Commonwealth of Pennsylvania, State of Georgia, State of Michigan, and State of Wisconsin, December 7, 2020. https://www.supremecourt.gov/DocketPDF/22/220155/163048/20201208132827887 TX-v-State-ExpedMot%202020-12-07%20FINAL.pdf
- ⁷⁵ The Superior Court Of Fulton County State Of Georgia, *Trump v. Raffensperger*, December 4, 2020. https://www.democracydocket.com/wp-content/uploads/sites/45/2020/12/Trump-v.-Raffensperger.pdf
- ⁷⁶ Liptak, Adam, "Supreme Court Allows Longer Deadline for Absentee Ballots in Pennsylvania and North Carolina," New York Times, October 28, 2020. https://www.nytimes.com/2020/10/28/us/supreme-court-pennsylvania-north-carolina-absentee-ballots.html
- ⁷⁷ Southwick, Ron, "Pa. received 10,000 ballots after polls closed on Election Day," *PennLive*, Nov10, 2020. https://www.pennlive.com/elections/2020/11/pa-received-10000-late-ballots-that-arrived-after-polls-closed-on-election-day.html
- ⁷⁸ Declaration of Jane Doe, Delaware County, Pennsylvania, November 7, 2020.
- ⁷⁹ The Supreme Court of Wisconsin, "Donald J. Trump et al v. Anthony Evers et al" December 1, 2020. https://cdn.donaldjtrump.com/public-files/press assets/wisconsin-filing-12-1-20 compressed.pdf
- 80 Declaration of Jane Doe, Oak Creek, Wisconsin, November 11, 2020.
- The Superior Court Of Fulton County State Of Georgia, *Trump v. Raffensperger*, December 4, 2020. https://www.democracvdocket.com/wp-content/uploads/sites/45/2020/12/Trump-v.-Raffensperger.pdf
- 82 Declaration of John Doe, Montgomery County, Pennsylvania, November 7, 2020.
- 83 Declaration of John Doe, Allegheny County, Pennsylvania, November 9, 2020.
- 84 Declaration of John Doe, Ingham County, Michigan, November 11, 2020.
- 85 Declaration of Jane Doe, Ingham County, Michigan, November 11, 2020.

```
<sup>86</sup> Declaration of Jane Doe, Wheaton, Illinois, November 9, 2020.
87 "Cure period of absentee and mail-in ballots," Ballotpedia, Accessed on December 14, 20.
https://ballotpedia.org/Cure period for absentee and mail-in ballots
88 "Cure period of absentee and mail-in ballots," Ballotpedia, Accessed on December 14,
https://ballotpedia.org/Cure period for absentee and mail-in ballots
<sup>89</sup> Declaration of Jane Doe, Centre County, Pennsylvania, November 11, 2020.
90 The United States District Court for the Middle District of Pennsylvania, Donald J. Trump for President et al v.
                  Boockvar
                                                                    November
                                                                                                         2020.
Kathy
                                                     al.
https://www.courtlistener.com/recap/gov.uscourts.pamd.127057/gov.uscourts.pamd.127057,169.0.pdf
<sup>91</sup> The United States District Court for the Middle District of Pennsylvania, Donald J. Trump for President et al v.
                                                                    November
https://www.courtlistener.com/recap/gov.uscourts.pamd.127057/gov.uscourts.pamd.127057.169.0.pdf
92 Declaration of Bartholomew W. and Jean B. W., Milwaukee County, Wisconsin, November 16, 2020. See Also
https://www.jsonline.com/story/news/2020/11/11/fact-check-republicans-claim-wisconsin-clerks-illegally-altered-
ballots/6234023002/
93 Declaration of John Doe, Delaware County Pennsylvania, November 9, 2020.
94 State of Michigan Court of Appeals, "Donald J. Trump for President et. al v. Jocelyn Benson," November 30, 2020.
https://www.democracydocket.com/wp-content/uploads/sites/45/2020/11/Trump-brief-FINAL.pdf
95 Affidavit of Jane Doe, Washtenaw County, Michigan, November 9, 2020.
        Cornell
                      University,
                                        "Equal
                                                      Protection,"
                                                                        Legal
                                                                                    Information
                                                                                                      Institute.
https://www.law.cornell.edu/wex/equal protection
97 Lai, Jonathan et al, "Joe Biden won 3 of every 4 mail ballots in Pennsylvania. Trump won 2 of 3 votes cast in
person.
                                                                future?"
            What
                     does
                              that
                                       mean
                                                 for
                                                        the
                                                                             The
                                                                                     Philadelphia
https://www.inquirer.com/politics/election/mail-ballots-pennsylvania-election-trump-biden-20201119.html
98 Declaration of John Doe, County of Milwaukee, Wisconsin, November 11, 2020
99 Blair County, Berks County, Lancaster County, Carbon County, Clinton County, Lycoming County, Dauphoin
County, and Perry County.
100 Joseph D. Hamm v. Kathy Boockvar, Commonwealth Court of Pennsylvania, November 3, 2020.
http://www.pacourts.us/assets/files/setting-7723/file-10362.pdf?cb=f327ff
<sup>101</sup> Secretary of State of Arizona, "Voters have a limited amount of time to correct certain ballot issues," November 9,
2020. https://azsos.gov/about-office/media-center/press-releases/1248
<sup>102</sup> In the United States District Court for the District of Arizona, Tyler Bowyer et al v.. Doug Ducey, December 2,
2020. https://www.democracydocket.com/wp-content/uploads/sites/45/2020/12/Bower-Complaint-AZ.pdf
National Conference of State Legislatures, "Poll Watchers and Challengers," October 1, 2020.
https://www.ncsl.org/research/elections-and-campaigns/poll-watcher-qualifications.aspx
<sup>104</sup> National Conference of State Legislatures, "Poll Watchers and Challengers," October 1, 2020.
https://www.ncsl.org/research/elections-and-campaigns/poll-watcher-qualifications.aspx
<sup>105</sup> Affidavit of Jane Doe, Rockdale County, Georgia, November 2020.
<sup>106</sup> Declaration of John Doe, Philadelphia, Pennsylvania, November 8, 2020.
<sup>107</sup> Affidavit of Jane Doe, Brookfield, Wisconsin, November 10, 2020.
          Ballotopedia,
                               "Voting
                                               Equipment
                                                                  and
                                                                             Methods
                                                                                              by
                                                                                                        State,"
https://ballotpedia.org/Voting methods and equipment by state
                               "Voting
          Ballotopedia,
                                               Equipment
                                                                 and
                                                                             Methods
                                                                                              by
                                                                                                        State,"
https://ballotpedia.org/Voting methods and equipment by state
110 Dominion Voting Systems, "About," https://www.dominionvoting.com/about/
111 Varnona, Frank "2020 Stolen Election by Dominion Voter Systems - Hammer & Scorecard," Conservative
Business Journal, https://www.conservativebusinessjournal.com/2020-stolen-election-hammer-and-scorecard/
                 Foundation.
                                "The
                                         Delian
                                                   Project."
                                                               https://www.clintonfoundation.org/clinton-global-
      Clinton
initiative/commitments/delian-project-democracy-through-technology
113 For example, the Chairman of Smartmatic, Mark Malloch-Brown, is on the board of George Soros' Open Society
Foundation. Open Society Foundation, "Leadership,"
                                                               https://www.opensocietyfoundations.org/who-we-
are/leadership/mark-malloch-brown
114 The First Judicial Court in Carson City, Nevada, "Jesse Law et al v. Judith Whitmer et al," November 17, 2020.
https://www.democracydocket.com/wp-content/uploads/sites/45/2020/11/nov-17-doc-2.pdf
115 The First Judicial Court in Carson City, Nevada, "Jesse Law et al v. Judith Whitmer et al," November 17, 2020.
https://www.democracydocket.com/wp-content/uploads/sites/45/2020/11/nov-17-doc-2.pdf
                                                                                                            34
```

of the signatures accompanying the mail-in ballots without ever having humanize inspect those signatures."

117 In the Superior Court of Arizona in and For the County of Maricopa, "Kelli Ward v. Constance Jackson et al."

November 24, 2020. https://assets.documentcloud.org/documents/20417265/ward-v-jackson-complaint-and-petition-for-discovery.pdf

¹¹⁸ In the Superior Court of Arizona in and For the County of Maricopa, "Kelli Ward v. Constance Jackson et al," November 24, 2020. https://assets.documentcloud.org/documents/20417265/ward-v-jackson-complaint-and-petition-for-discovery.pdf

Affidavit of John Doe, Dallas County, Texas. November 17, 2020. https://www.courtlistener.com/recap/gov.uscourts.gand.283580/gov.uscourts.gand.283580.7.1 2.pdf

Ramsland Jr., Russell. "Antrim Michigan Forensics Report." William Bailey v. Antrim County, Michigan, December 13, 2020.

https://depernolaw.com/uploads/2/7/0/2/27029178/antrim_michigan_forensics_report_[121320]_v2_[redacted].pdf

121 "Excerpts from the 2002 FEC Voting System Standards – 3.2.1 Accuracy Requirements." Michigan Secretary of

State. https://www.michigan.gov/sos/0,4670,7-127-1583-130621--,00.html

"Document Retention Schedule." Michigan Bureau of Elections, May 2019. https://www.michigan.gov/documents/sos/Document Retention Schedule 412493 7.pdf

Paul. "Georgia voting irregularities: The curious case of Biden's 20,000-vote surge." *The Citizen*, November 15,2020. https://thecitizen.com/2020/11/15/georgia-voting-irregularities-the-curious-case-of-bidens-20000-vote-surge/

Parks, Miles, "Why Some Mail-In Ballots Are Rejected As Invalid," NPR, October 4, 2020. https://www.npr.org/2020/10/04/920175418/why-some-mail-in-ballots-are-rejected-as-invalid

¹²⁵ Livingston, Doug, "Why absentee ballots get rejected, and how to make yours count," *USA Today*, September 21, 2020. https://www.beaconjournal.com/story/news/2020/09/21/why-absentee-ballots-rejected-presidential-and-other-elections/3486553001/

¹²⁶ Livingston, Doug, "Why absentee ballots get rejected, and how to make yours count," *USA Today*, September 21, 2020. https://www.beaconjournal.com/story/news/2020/09/21/why-absentee-ballots-rejected-presidential-and-other-elections/3486553001/

127 Election Assistance Commission, "The Election Administration and Voting Survey; A Report to the United States Congress," 2016. https://www.eac.gov/sites/default/files/eac_assets/1/6/2016_EAVS_Comprehensive_Report.pdf

128 Ballotopedia, "Election results, 2020: Analysis of rejected ballots," December 11, 2020. https://ballotpedia.org/Election_results, 2020: Analysis of rejected ballots

See Also

Office of Nevada Secretary of State Barbara K. Cegavske, "2020 General Election Turnout Mail Ballot Information," https://www.nvsos.gov/sos/home/showdocument?id=9058

129 Election Assistance Commission, "The Election Administration and Voting Survey; A Report to the United States Congress," 2016. https://www.eac.gov/sites/default/files/eac_assets/1/6/2016_EAVS_Comprehensive_Report.pdf

Ballotopedia, "Election results, 2020: Analysis of rejected ballots," December 11, 2020. https://ballotpedia.org/Election results, 2020: Analysis of rejected ballots
See Also

U.S. Elections Project, "Pennsylvania Early Voting Statistics," November 20, 2020. https://electproject.github.io/Early-Vote-2020G/PA.html

131 Election Assistance Commission, "The Election Administration and Voting Survey; A Report to the United States Congress," 2016. https://www.eac.gov/sites/default/files/eac_assets/1/6/2016_EAVS_Comprehensive_Report.pdf

The Superior Court Of Fulton County State Of Georgia, *Trump v. Raffensperger*, December 4, 2020. https://www.democracydocket.com/wp-content/uploads/sites/45/2020/12/Trump-v.-Raffensperger.pdf

133 For example, in Pennsylvania, 3 out of every 4 absentee/mail-in ballots went to Joe Biden https://www.inquirer.com/politics/election/mail-ballots-pennsylvania-election-trump-biden-20201119.html

And in Milwaukee, Wisconsin, 84% of absentee/mail-in ballots went to Joe Biden

https://www.tmj4.com/news/election-2020/no-joe-biden-did-not-get-100-percent-of-all-milwaukee-absentee-ballots ¹³⁴ Heine, Debra, "Mathematician Says Biden May Have Received 130 Percent of the Democrat Vote in Maricopa County, Arizona," December 2, 2020. https://themichiganstar.com/2020/12/02/mathematician-says-biden-may-have-received-130-percent-of-the-democrat-vote-in-maricopa-county-arizona/

Affidavit of Russel R., Dallas County, Texas. November 17, 2020. https://www.courtlistener.com/recap/gov.uscourts.gand.283580/gov.uscourts.gand.283580.7.1 2.pdf

- ¹³⁶ Milwaukee City Wire News Service, "Analysis: Five Milwaukee wards report 89% turnout in 2020 presidential vote; Biden nets 146K votes in city," November 4, 2020. https://mkecitywire.com/stories/564495243-analysis-seven-milwaukee-wards-report-more-2020-presidential-votes-than-registered-voters-biden-nets-146k-votes-in-city
- ¹³⁷ Milwaukee City Wire News Service, "Analysis: Five Milwaukee wards report 89% turnout in 2020 presidential vote; Biden nets 146K votes in city," November 4, 2020. https://mkecitywire.com/stories/564495243-analysis-seven-milwaukee-wards-report-more-2020-presidential-votes-than-registered-voters-biden-nets-146k-votes-in-city
- Duda, Jeremy. "GOP lawsuit questions 'duplicate' ballots in Queen Creek," San Tan Valley Sentinel, November 27, 2020. https://www.pinalcentral.com/san_tan_valley_sentinel/local_news/gop-lawsuit-questions-duplicate-ballots-in-queen-creek/article_ee9557d0-97e4-53e9-a269-5beb4b64370a.html
- ¹³⁹ In the Superior Court of Arizona in and For the County of Maricopa, *Kelli Ward v. Constance Jackson et al*, November 24, 2020. https://assets.documentcloud.org/documents/20417265/ward-v-jackson-complaint-and-petition-for-discovery.pdf
- ¹⁴⁰ Voter Integrity Project, "Anomalies in Vote Counts and Their Effects on Election 2020," November 24, 2020. https://votepatternanalysis.substack.com/p/voting-anomalies-2020
- ¹⁴¹ Voter Integrity Project, "Anomalies in Vote Counts and Their Effects on Election 2020," November 24, 2020. https://votepatternanalysis.substack.com/p/voting-anomalies-2020
- ¹⁴² Voter Integrity Project, "Anomalies in Vote Counts and Their Effects on Election 2020," November 24, 2020. https://votepatternanalysis.substack.com/p/voting-anomalies-2020
- ¹⁴³ News Now, "Michigan Republican Electors Harassed And Forced To Change Vote," November 18, 2020. https://www.youtube.com/watch?v=YW1YzQY 1Ro
- Dowling, M. "Michigan's largest county refuses to certify the election Update, evil wins," *Independent Sentinel*, November 17, 2020. https://www.independentsentinel.com/michigans-largest-county-refuses-to-certify-the-election/ See Also
- Institute for Political Economy, "Wayne County Michigan Withdraws Election Certification, Security Expert Concludes Michigan Was Stolen." https://www.newsbreak.com/news/2105758771365/wayne-county-michigan-withdraws-election-certification-security-expert-concludes-michigan-was-stolen
- Pentchoukov, Ivan, "Illegal Money-For-Votes Raffles Conducted in Several States in 2020 Election," December 1, 2020. https://www.theepochtimes.com/illegal-money-for-votes-raffles-conducted-in-several-states-in-2020-election 3598915.html
- Ballotopedia, "Partisan composition of state legislatures," December 4, 2020. https://ballotpedia.org/Partisan composition of state legislatures
- 146 State of Texas v. The Commonwealth of Pennsylvania, State of Georgia, State of Michigan, State of Wisconsin, "Motion for Leave to File Bill of Complaint," December 7, 2020. https://www.supremecourt.gov/DocketPDF/22/220155/162953/20201207234611533 TX-v-State-Motion-2020-12-07%20FINAL.pdf pg. 1
- ¹⁴⁷ State of Texas v. The Commonwealth of Pennsylvania, State of Georgia, State of Michigan, State of Wisconsin, "Motion for Leave to File Bill of Complaint," December 7, 2020. https://www.supremecourt.gov/DocketPDF/22/220155/162953/20201207234611533 TX-v-State-Motion-2020-12-07%20FINAL.pdf pg. 1
- 148Ballotopedia, "Partisan composition of state legislatures," December 4, 2020. https://ballotpedia.org/Partisan composition of state legislatures

Exhibit 80

BTC/USD 32223.96 +218.08 (+0.68%)



ETH/USD 1050.44 +7.49 (+0.72%)



S&P 500 3706.8 +1.1 (+0.03%)



WORLD

POLITICS

LATINO

EN ESPAÑOL

VIDEO: Sidney Powell Wants to Fight for Donald Trump — But His Aides Won't Let Her, She Says

Does Sidney Powell have a job defending Trump? "That is a good question!"

By David Martosko December 27, 2020 Political Campaigns



Attorney Sidney Powell said in a Dec. 23, 2020 interview that senior White House aides are keeping her from helping President Donald J. Trump prove that widespread voter fraud cost him re-election. Powell is pictured in a screen-grab from video shot at the Trump International Hotel in Washington, D.C. (Chris Winter/Zenger News)

President Donald J. Trump says he wants a lawyer to probe "election theft," but the president's leading candidate, Sidney K. Powell, says she has been barred from the White House by the president's own chief of staff.

While Powell and the president discussed the role last Friday in a contentious four-and-a-halfhour Oval Office meeting, she says, insiders opposed her appointment, sometimes shouting defiantly at the president. Powell's on-the-record account reveals a White House riven by internal feuding, and a growing divide between the president's most senior staff and his most devoted outside supporters.



TRENDING NOW







Take Up Plight of India's Farmers in Letter to Pompeo



Delegation Takes Measure of Political Situation in Nepal



India Approves Two Vaccines for **Emergency Use**



RECENT UPDATES



Terrorist Killing of Hazara Shiites in Balochistan



This Is How Latin America Receives the Three Wise Men



internal feuding, and a growing divide between the president's most senior staff and his most devoted outside supporters.



By Saturday morning, Powell says, the president's most senior aides had declined to give her a Secret Service-issued pass to come and go from the West Wing. "I've been blocked from speaking to or communicating with the president since I left the Oval Office on Friday night," she says, "by apparently everyone around him."



Terrorist Killing of Hazara Shiites in Balochistan

This Is How Latin America Receives the Three Wise



Black Colleges Use **Esports to Attract** Students and Hook them on Science and Engineering

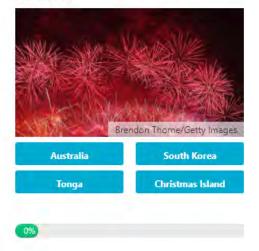


and the Crack King of New York - and Now He's on YouTube

The Smarter News Quiz



Which of these countries celebrates the New Year earlier than the rest of the world?





During the Zenger interview, conducted on video in a 7th-floor suite at the Trump International Hotel in Washington DC, Powell said she has had no contact with Trump since the Dec. 18 meeting.

White House Press Secretary Kayleigh McEnany declined to comment on the record about whether any senior officials, including Chief of Staff Mark R. Meadows, National Security Advisor Robert C. O'Brien and White House Counsel Pat A. Cipollone, have intervened to keep Powell out of the White House, All three participated in Friday's meeting, which devolved into

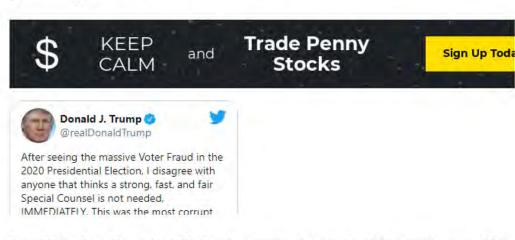
ZENGER

the Dec. 18 meeting

White House Press Secretary Kayleigh McEnany declined to comment on the record about whether any senior officials, including Chief of Staff Mark R. Meadows, National Security Advisor Robert C. O'Brien and White House Counsel Pat A. Cipollone, have intervened to keep Powell out of the White House. All three participated in Friday's meeting, which devolved into chaos and finger-pointing about who was—or was not—serving Trump's interests. Powell confirmed that former National Security Advisor Gen. Michael T. Flynn accompanied her to the Oval Office.

O'Brien and Trump's personal lawyer Rudolph S. Giuliani participated via telephone. Other aides walked in and out of the Oval Office periodically; they could not be identified by Zenger's reporting. A message to Giuliani seeking comment was not returned. Asked to confirm Giuliani took part, his attorney Bob Costello said, "I don't know the answer to that."

Trump said Tuesday in a videotaped statement that he would "pursue every legal and constitutional option available to stop the theft of the presidential election." He tweeted Wednesday, "I disagree with anyone that thinks a strong, fast, and fair Special Counsel is not needed, IMMEDIATELY. This was the most corrupt election in the history of our Country, and it must be closely examined!" Only the U.S. attorney general can appoint a special counsel, but the president can appoint a special White House counsel who would have more limited powers and protections.



Does Sidney Powell have that job? "That is a good question!" she told Zenger News, laughing. She says she was verbally offered the job, but that senior officials from the Office of White House Counsel have prevented her from presenting the president with paperwork to make it official.

Meanwhile, she says, Meadows and others have blocked permission for her to visit the executive mansion or its nearby buildings. Senior officials have "thrown sand in the gears" of actions the president asked her to carry out, she says.

Powell challenged the accuracy of the anonymous accounts that appeared in major news outlets. There was no talk of "martial law," or sending soldiers to seize ballot machines, she said, or holding a second round of elections in swing states. "I can tell you for sure," she said, "that was not discussed in the Oval Office Friday night."

Flynn said his recollection of the meeting matches Powell's. "No one talked about martial law, no matter what some of the news reports say," he told Zenger.

The Smarter News Quiz



Which of these countries celebrates the New Year earlier than the rest of the world?



OFFBEAT SCIENCE WCRLD POLITICS LATINO EN ESPAÑOL VIDEO

There was no talk of "martial law," or sending soldiers to seize ballot machines, she said, or holding a second round of elections in swing states. "I can tell you for sure," she said, "that was not discussed in the Oval Office Friday night."

Flynn said his recollection of the meeting matches Powell's. "No one talked about martial law, no matter what some of the news reports say," he told Zenger.

Such an appointment would hand Powell a top-level security clearance and 24-hour access to the White House, and likely put her in the same office suite as the White House Counsel privileges she says some of the men who work closest to the Oval Office do not want her to have.

"It has not come to pass," Powell says, "because it seems it was blocked after Friday night, or undone, or I'm not sure what you'd call it" by senior White House staff including, she suggested, Meadows and Cipollone.

Cipollone, Meadows and O'Brien argued strenuously against hiring Powell, she says, and warned of sharply negative reactions among the Washington-based press corps, and among members of Congress whose support Trump would need in the coming weeks if he had any hope of reversing the November 3 election results that made former Vice President Joseph R. Biden his successor-in-waiting.

Powell said intramural feuding squanders time that could be spent on investigations and court filings. "Sidney is a fantastic advocate," Flynn said. "You know how POTUS says you should never give up no matter what? That's Sidney. And that's fantastic. We need more like her."

Powell says her small team of privately funded attorneys are "still collecting evidence through fire hoses," and that "thousands and thousands of people have stepped forward and given sworn statements" about irregularities they say they witnessed on Election Day. Powell declined to provide any new evidence of voter fraud, instead referring to previously published claims in a binder of material her staff provided to Zenger News two hours before the Dec. 23 interview. (You can read it here.)



The Smarter News Quiz



Which of these countries celebrates the New Year earlier than the rest of the world?



ZENGER OFFBEAT SCIENCE WORLD POLITICS BUSINESS TECH URBAN LATING OF ESPAÑOL VIDEO



Sidney Powell flipped through a binder of materials which she says prove her case that widespread voter fraud cost President Donald J. Trump re-election. Powell is pictured during a Dec. 23 interview at the Trump International Hotel in Washington, D.C. (Claire Swift/Zenger News)

Powell cited reports by the FBI and the Cybersecurity and Infrastructure Security Agency in October 2020 warning that Iran-backed hackers were "likely intent on influencing and interfering with the U.S. elections." One report was updated on Election Day, saying the unnamed Iranians had infiltrated election websites and stolen voter registration data, later launching a "mass dissemination of voter intimidation emails to U.S. citizens."

That same agency issued a Nov. 12 statement that "[t]he November 3rd election was the most secure in American history"—apparently undercutting Powell's claims.

A similar federal report also cast doubt. "There is no evidence that any voting system deleted or lost votes, changed votes, or was in any way compromised," said the executive committee of the inter-agency Election Infrastructure Government Coordinating Council. That panel, formed in 2017 as claims swirled that Russia had infiltrated the 2016 election to benefit Trump, includes officials from the Cybersecurity and Infrastructure Security Agency, the U.S. Election Assistance Commission, the National Association of Secretaries of State, the National Association of State Election Directors (NASED), the nonprofit Democracy Works and Electronic Registration Information Center and companies whose hardware and software are used in U.S. elections.

The Smarter News Quiz



Which of these countries celebrates the New Year earlier than the rest of the world?



Australia

South Korea

Tonga

Christmas Island



Election Assistance Commission, the National Association of Secretaries of State, the National Association of State Election Directors (NASED), the nonprofit Democracy Works and Electronic Registration Information Center and companies whose hardware and software are used in U.S. elections.

Powell on Wednesday did point to a little-known opinion issued Oct. 11 by federal judge Amy Totenberg, whom she mistakenly referred to as Nina Totenberg—the name of the National Public Radio host. (The two women are sisters.) Judge Totenberg, who sits on the U.S. District Court for the Northern District of Georgia, cited a risk of "stealth vote alteration or operational interference" in touchscreen voting devices sold by Dominion Voting Systems if they are not properly audited.



Those risks "are neither hypothetical nor remote under the current circumstances," Totenberg wrote, adding that the machines can "deprive voters of their cast votes" by storing data in unverified digital QR codes, making any potential manipulation invisible to voters "at least until any portions of the system implode because of system breach, breakdown, or crashes."

Powell says those exact kinds of crashes during vote-counting allowed Democratic election officials to begin "backfilling their vote [totals] with fraudulent ballots" while Dominion machines were disabled. "We can definitely show that the election system was sufficiently tampered with, with the aid of foreign influence, to flip any number of states," she says.



Powell did not provide any evidence that the potential fraud Judge Totenberg identified in October materialized as actual fraud in November.

The Smarter News Quiz



Which of these countries celebrates the New Year earlier than the rest of the world?



Christmas Island



Tonga

This claim about election fraud is disputed

Powell did not provide any evidence that the potential fraud Judge Totenberg identified in October materialized as actual fraud in November.

Powell wants Trump to order federal authorities to secure voting machines from both Republican- and Democrat-heavy districts in swing states, conduct forensic audits, and find out whether any of them were connected to the Internet on Election Day. Such Internet connections might allow remote actors to tamper with vote totals in real time.

Ballots on such Internet-linked machines, she says, are "invalid."

As Americans prepared to mark Christmas Eve on Thursday, Trump tweeted from his Mar-a-Lago resort in Palm Beach Florida: "VOTER FRAUD IS NOT A CONSPIRACY THEORY, IT IS A FACT!!!"

(Edited by Richard Miniter and Claire Swift. Videography by Chris Winter.)

The Smarter News Quiz



Which of these countries celebrates the New Year earlier than the rest of the world?



Australia

South Korea

Tonga

Christmas Island



You May Like



Dark Spots On Your Face? Here's How To Clear Them Fast

Gundry MD



1 Odd Trick Restores Your Eyes To Perfect 20/20 Vision

Complete Vision Formula



Man Who Predicted 2020 Crash Says "Now Is The Time"

The Legacy Report



Surgeon Reveals How To Fill In Balding Eyebrows

Beverly Hills MD



Medicare Recipients Are In For A Big Surprise This January

Finance Daily



New Method Traces Ancestry Back Thousands of Years

CRI Genetics Digest

NEXT POST ** 84 Years After His Spanish Civil War

PREVIOUS POST VIDEO: Hidden Depths: Divers Discover VIDEO: Woman Hugs Father's Remains 17th-Century Wooden Merchant Vessel

Lago resort in Palm Beach Florida: "VOTER FRAUD IS NOT A CONSPIRACY THEORY, IT IS A FACT!!!"

(Edited by Richard Miniter and Claire Swift. Videography by Chris Winter.)

The Smarter News Quiz



You May Like



Dark Spots On Your Face? Here's How To Clear Them Fast

Gundry MD



1 Odd Trick Restores Your Eves To Perfect 20/20 Vision

Complete Vision Formula



Man Who Predicted 2020 Crash Says "Now Is The Time"

The Legacy Report





Surgeon Reveals How To Fill In Balding Eyebrows

Beverly Hills MD



Medicare Recipients Are In For A Big Surprise This January

Finance Daily



New Method Traces Ancestry Back Thousands of Years

CRI Genetics Digest

Which of these countries celebrates the New Year earlier than the rest of the world?



Australia

South Korea

Tonga

Christmas Island



PREVIOUS POST VIDEO: Hidden Depths: Divers Discover VIDEO: Woman Hugs Father's Remains 17th-Century Wooden Merchant Vessel

NEXT POST ** 84 Years After His Spanish Civil War Execution









© Z News Service, Inc. 2020. All Rights Reserved. 2303 Ranch Road, 620 South, Suite 160-125, Austin, Texas 78734

About Us

Press

Ethics

Corrections

Who was John Peter Zenger?

Register

Contact Us

FAQ

Privacy Policy

Terms & Conditions

Trademarks

Exhibit 81

2020 ELECTION EVIDENCE OF FOREIGN INTERFERENCE

SIDNEY POWELL

AUTHOR OF THE BESTSELLER LICENSED TO LIE

About
Court Filings / Evidence
News SCOTUS Shop



Search

Evidence of Foreign Interference in the 2020 Election

OUTLINE

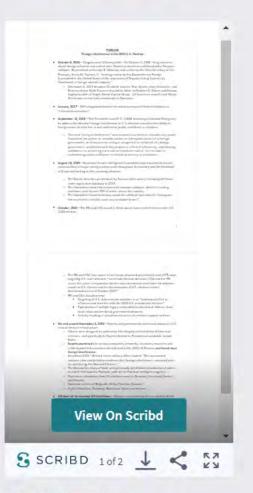
TEACH POINT & CUTSAN From the Control of the CutsAnd Annual Contr

SUMMARY



Summary by Sidney Powell

TIMELINE



Timeline by Sidney Powell

Outline by Sidney Powell

EVICIENCE OT FOREIGN INTERFERENCE IN THE ZUZU
Case 1:21-cv-00040 Socument 1-80 Filed 01/08/21 Page 3 of 3

Election

OUTLINE

SUMMARY

TIMELINE







Outline by Sidney Powell

Summary by Sidney Powell

Timeline by Sidney Powell

Fighting to expose the truth.

Privacy Policy | Terms & Conditions

Copyright © 2021 Sidney Powell

Contact
Invite To Speak
Support
Shipping &
Returns

Exhibit 82

THE FOLLOWING ESTABLISHES "FOREIGN INTERFERENCE" IN THE UNITED STATES 2020 ELECTIONS AS DEFINED IN E.O. 13848

"...any covert, fraudulent, deceptive, or unlawful actions or attempted actions of a foreign government, or of any person acting as an agent of or on behalf of a foreign government, undertaken with the purpose or effect of influencing, undermining confidence in, or altering the result or reported result of, the election, or undermining public confidence in election processes or institutions."

- Definition of "foreign interference" with respect to an election per Executive Order 13848 (2018).

The President of the United States, pursuant to the Constitution and laws of the United States of America, including Article 2 section 1 of the U.S. Constitution, Executive Orders 12333 and 13848, National Security Presidential Memoranda 13 and 21, the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) (IEEPA) and all applicable Executive Orders derived therefrom, the National Emergencies Act (50 U.S.C. 1601 et seq.) (NEA), and section 301 of title 3, United States Code, has already found a national emergency regarding the elections since 2018. The following list is of evidence and findings already made of foreign

interference in the November 2020 General Election—especially by Iran.¹ There is additional evidence developing of foreign interference from China.

On September 12, 2018, through Executive Order 13848, the President declared a national emergency to address the threat of foreign interference in a United States election based on findings that the ability of persons outside the United States to interfere with or undermine public confidence in United States elections, including through the unauthorized accessing of election and campaign infrastructure or the covert distribution of propaganda and disinformation, constituted an unusual and extraordinary threat to the national security and foreign policy of the United States.

There is now clear and definitive evidence of both foreign interference and widespread election fraud impacting processes and critical infrastructure before, during and after the US General Election of November 3, 2020. Additional evidence of foreign election interference surfaces daily.

As the FBI and CISA (Cybersecurity and Infrastructure Security Agency) have already found with respect to this election, these unprecedented attacks on critical election infrastructure are designed to undermine the integrity and reliability of

1

American elections, and thereby strike at the heart of this Republic. Such malicious activity is destabilizing and detrimental to the national security, economic security, and foreign policy of the United States. Urgent action is necessary to secure and preserve U.S. election systems, and additional forensic assessment should be conducted immediately to determine the full extent of foreign interference and unauthorized access to critical election infrastructure.

These challenges we now face as a nation have been compounded by censorship and disinformation campaigns of foreign and domestic adversaries, in combination with social media companies, "news" outlets, and search engines. Collectively, these entities have engaged in systematic censorship of information – specifically, evidence of foreign interference and widespread fraud and criminal activity in the 2020 General Election, while actively spreading misinformation about these matters of national importance, thereby facilitating the destabilization of the American political process.

A sampling of evidence and information concerning foreign election interference and related matters is therefore included below for the public benefit. The evidence shows:

a) There was foreign interference in the November 3, 2020 election.

Foreign interference was observed and documented by experts and data analysts, including the Federal Bureau of Investigation (FBI) and Cybersecurity and Infrastructure Security Agency (CISA). Multiple expert witnesses and cyber experts identified acts of foreign interference in the

- election in the days immediately prior to November 3, 2020 and continuing in the following weeks.
- b) Election machines and software used by most voters across the country are compromised. The five companies which provide systems that control voting in the United States are Dominion, ES & S, Hart InterCivic, Sequoia, and Smartmatic. The three largest vendors Dominion, ES & S, and Hart InterCivic collectively provide machines and software for over 90% of all eligible U.S. voters. The numerous similarities between these voting systems are related to shared origin of the software code, and all of the systems have similar security and functional flaws.
- c) Individuals and firms that are foreign (or which have substantial foreign ties) own or control each of these vendors. Additionally, approximately 20% of the components used in these voting machines are from China-based companies. In addition, there is currently evidence of direct interference from China in the Georgia run-off elections.
- d) These election systems appear to have been intentionally and purposefully designed with inherent errors to create systemic fraud and influence election results.

The President is the Chief Law Enforcement Officer and Commander in Chief of the United States of America. It is the duty of the President to protect and defend the Constitution and laws of the United States. This requires taking action to protect national security and the country's critical infrastructure, including the security and

integrity of our voting systems necessitated by foreign interference in the November 3, 2020 elections.

Consistent with these facts findings, and his sworn duty as President, the President should invoke all authorities to act to protect the Republic of the United States of America, the country's critical election and cyber infrastructure, election integrity, and all related national interests, and pursuant to Executive Order 13848, immediately take all legal action appropriate and within the power of the President to determine the true legal votes and outcome of this election.

HIGHLIGHTS OF THE EVIDENCE

- 1) The Bipartisan Report of the Senate Intelligence Committee issued on August 18, 2020 warned of the known vulnerabilities of major voting systems used throughout the country and the likelihood of fraud and hacking in the upcoming elections.
 - a) According to the report, beginning by at least 2014, "the Russian government directed extensive activity against the U.S. election infrastructure," but there was "no evidence any votes were changed or voting machines manipulated."
 - b) The Department of Homeland Security designated the "election infrastructure" of the United States as a "Critical Infrastructure Subsector." See SSCI Report: 3 and n. 1 (2018).
 - c) By the end of 2018, "the Russian cyber actors had successfully penetrated Illinois' voter registration database, viewed multiple database tables, and accessed up to 200,000 voter registration records." SSCI Report: 22 (2018).

- d) In 2018, "Congress appropriated \$380 million in grant money for the states to bolster cybersecurity and replace vulnerable voting machines." SSCI Report: 5
- e) The SSCI found ample evidence to suggest that the Russian government was developing and implementing capabilities to interfere in the 2016 elections, including undermining confidence in the elections.
- f) GEMS Software is common to each of these voting systems. GEMS has been owned by Dominion since 2010, when an antitrust suit brought by then-Attorney General Eric Holder ended with the divestiture of Diebold's Premier division and its acquisition by Dominion was approved by the Department of Justice.
- g) "ES & S Voting Systems disclosed that some of its equipment had key security vulnerability. ES & S installed remote access software on machines it sold in the mid-2000s, which . . . created potential remote access into the machines." SSCI Report: 41. Three hundred voting jurisdictions used the software, and 41 states used it products. Id.
- h) The Committee heard disturbing testimony of the ability of operators to "reprogram the machine to invisibly cause any candidate to win." Id. At 42. It is undisputed that the FBI and the National Security Division of the DOJ knew of these national security issues and threats. Id. At 43.
- i) The Committee identified problems with vendors, supply chains, the absence of any regulatory authority requiring vendors to adhere to basic security practices. "If there is no way to audit the election, that is absolutely a

national security concern." Minority Views of Senator Wyden, Report: 2 (2018). Notably, Dominion Voting Systems do not maintain a truly auditable trail for a number of reasons, among them being that its audit logs are editable by operators (and by those with unauthorized access).

j) Dominion is used in 22 states and 600 local jurisdictions. For example, in the Summer 2019, the State of Georgia purchased Dominion Voting Systems for its operations state-wide at a contract price of \$107 million.

2) Dominion Voting Systems and Scytl/Clarity Elections:

- a) Dominion Voting Systems is owned and controlled by foreign entities. As a National Security concern, having foreign entities managing US elections gives foreign actors strategic but hidden influence upon the future of foreign policy, National Security Strategy, and National Military Strategy. Since these companies move data around the world, malign foreign states, and actors or even opportunistic foreign states and actors have ability to influence (or even determine) election outcomes in ways that are most favorable to their government or causes. This impacts all the elements of US National Security; Diplomacy; Information; Military; Economic; Financial; Intelligence; and Law Enforcement (DIMEFIL).
- b) It is a fact that the US institutions listed above are under constant cyberattack. Attacking the election system to control the administration taking

- power of the largest economy in the world is a singular assault on all of the DIMEFIL pillars of national power at once.
- c) Electronic data from US elections was transmitted to Germany, Barcelona, Serbia, and Canada.
 - i) **Dominion Servers** in Belgrade Serbia. P 82.117.198.54 (ASN Range: 82.117.192.0/19)
 - ii) **Dominion Servers** ftp.dominionvoting.com with IP 69.172.237.100 (ASN Range: 69.172.236.0/22) is located in Toronto, Canada
 - iii) The website www.scytl.com with IP 52.57.209.147 (ASN Range: 52.57.0.0/16) is (was) located in **Frankfurt Germany.**
 - iv) The website support.scytl.com with IP 213.27.248.118 (ASN Range: 213.27.128.0/17) is located in **Barcelona**, **Spain**
 - v) The website scytl-com.mail.protection.outlook.com with IP 104.47.10.36 (ASN Range: 104.40.0.0/13) is located in **Ireland.**
- d) Dominion Voting Systems and related companies are owned or heavily controlled and influenced by foreign agents, countries, and interests.
- e) The forensic report prepared for Antrim County, Michigan found that, "the Dominion Voting System is intentionally and purposefully designed with inherent errors to create systemic fraud and influence election results".
 - i) For example, the report found that the system intentionally generates an enormously high number of ballot errors. The intentional errors lead to

- individual or bulk adjudication of ballots with no oversight, no transparency, and no audit trail.
- ii) Dominion operating system has control functions to allow for transfer of adjudication files from one Results Tally system to another. This is the exact type of issue that leads to voter and/or election fraud.
- iii) The report found the election management system to be wrought with unacceptable vulnerabilities—including access to the internet— a key indicator to find evidence of fraud, and numerous malicious actions.
- f) On election night the DE-CIX Frankfurt ("The World's Leading Internet Exchange") experienced a significant spike over its previous high traffic peaks. One expert attributed the likely cause to increased data flow to servers supporting the US Election. On November 4, 2020, the firm wrote, "Last night, for the first time, we reached 10 Terabits per second peak traffic at DE-CIX Frankfurt." (cf. https://www.de-cix.net/en/about-de-cix/news/de-cix-frankfurt-hits-10-tbps-peak-traffic)
- 3) The numerous similarities among these voting systems are related to common software code.
 - a) Further forensic investigation will confirm that Dominion Voting Systems,
 Smartmatic, Electronic Systems & Software, and Hart Inter Civic, all have
 similar security and functional flaws. Clarity Election Night Reporting,

Edison Research, Scytl have serious vulnerabilities that were subject to foreign interference in the 2020 election in the United States.

- b) These systems bear the same crucial code "features" and defects that allowed the same outside and foreign interference in the 2020 US General Election, in which votes were in fact altered and manipulated contrary to the will of the voters, as evidenced by the forensic analysis of Antrim County MI as well as statements of citizens there who witnessed machine alteration of election results.
- c) Each of the companies use EML (Election Markup Language) and are susceptible to cross site scripting attacks (XSS) as described on page 7 in the Joint Cybersecurity Advisory. Cross-site scripting (also known as XSS) is a web security vulnerability that allows an attacker to compromise the interactions that users have with a vulnerable application. It allows an attacker to circumvent the same origin policy, which is designed to segregate different websites from each other. Cross-site scripting vulnerabilities normally allow an attacker to masquerade as a victim user, to carry out any actions that the user is able to perform, and to access any of the user's data. If the victim user has privileged access within the application, then the attacker might be able to gain full control over all of the application's functionality and data.
- d) Most, if not all, related sites were created using WordPress. WordPress currently has 2,675 CVE (Common Vulnerabilities and Exposures) listed on cve.mitre.org.

- e) Experts performed an OpenVAS Vulnerability assessment for both Dominion and Scytl. There were multiple issues related to out-of-date plugins and themes, which leaves sites vulnerable to attack.
- f) Dominion's purchase of Sequoia Voting Systems from Smartmatic has resulted in the same "Source Code" being used today. Due to this and various other mergers, acquisitions, licensing agreements and partnerships, the entire election ecosystem in the United States is convoluted, murky and hidden. This began with the Venezuelan investment into Smartmatic specifically to rig elections. It should also be noted that Smartmatic still runs elections in the US and licenses its software to other Election Management System Companies.
- g) The refusal to inspect software code goes against common US legal and business practice. It is common legal procedure to inspect code under a protective order to determine intellectual property suits. The claims from all of these companies that their code should not be inspected is a strong indicator of malign activity.
- h) During a recent forensic audit, experts discovered WinEDs and GEMS in the Dominion Voting System EMS (Election Management System). Both of those modules have been included in adverse findings from the EAC but are still in use today.

- i) Dominion and Smartmatic share a physical address in Barbados despite their insistence that there is no relationship between the companies. They also have a mutual non- compete agreement detailing shared resources and code.
- j) The fact that a Smartmatic board member, Peter Neffenberger, is named as a key member of the presidential transition team is a significant conflict of interest. Additionally, members of George Soros' Open Society Foundations are also serving board members of Smartmatic.
- k) Dominion Voting Systems is based in Toronto, Canada, and assigns its intellectual property including patents on its firmware and software and trademarks to Hong Kong and Shanghai Bank Corporation (HSBC), a bank with its foundation in China and its current headquarters in London, United Kingdom.
- l) Given the overlap between Dominion and Smartmatic, including the shared business address in Barbados, the FCC Report ID: 2AGVK-VIU811 issued by the CCIS Lab in Shenzhen, China is very concerning. The **Voter Identification Unit** report was issued on July 23, 2020 and would give China insight on how to exploit the voting machines used in the US Election.

4) Multiple expert witnesses and cyber experts identified acts of foreign interference in the election prior to November 3, 2020 and continued in the following weeks.

- a) There is evidence of a massive cyber-attack by foreign interests on our crucial national infrastructure surrounding our election—not the least of which was the hacking of the voter registration system by Iran. (E.O. 13800 of May 11, 2017). This is compounded by the magnitude of the Solar Winds exploit that has exposed the private, public and government related companies and agencies. This includes the companies and agencies directly involved with securing our elections.
- b) The FBI and CISA issued a joint Cybersecurity Advisory on October 30, 2020 (Report ID: AA20-304A). This joint cybersecurity advisory was coauthored by the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI). CISA and the FBI are aware of an Iranian advanced persistent threat (APT) actor targeting U.S. state websites—to include election websites. CISA and the FBI assess this actor is responsible for the mass dissemination of voter intimidation emails to U.S. citizens and the dissemination of U.S. election-related disinformation in mid-October 2020.¹ (Reference FBI FLASH message ME-000138-TT, disseminated October 29, 2020). Further evaluation by CISA and the FBI has identified the targeting of U.S. state election websites was an intentional effort to influence and interfere with the 2020 U.S. presidential election.

5) Staple Street Partners

a) Staple Street Partners is an equity firm that owns Dominion Voting Systems.

- b) Hootan Yaghoobzadeh is the CEO and Chairman of Staple Street Capital, which is the entity that owns Dominion. Yaghoobzadeh was a close confidant to Sadaam Hussein and worked for the Saudi Bin Laden group. He previously worked at the Carlyle Group and Cerberus Capital Management.
- c) Dominion Voting Systems based in Toronto entered into a Security Agreement with HSBC Bank on September 25, 2019, assigning all intellectual property and assets including Trademarks, Patents and Software (see below).
- d) On October 8, 2020, \$400,000,000 from UBS Securities a Chinese managed subsidiary of UBS Global AG was invested in Dominion Voting Systems.
- 6) Since at least 2006, members of Both Parties have complained of defective voting system, especially Dominion Voting Systems.
 - a) On October 6, 2006, citing concerns about foreign influence and control over Dominion machines and Smartmatic/Sequoia software, Representative Carolyn B. Maloney sent a letter to the then-Secretary of the Treasury, Henry M. Paulson, Jr. "seeking review by the Committee on Foreign Investment in the United States of the acquisition of Sequoia Voting Systems by Smartmatic, a foreign-owned company." Rep. Maloney explained her view that "this issue demands the most thorough independent investigation by CFIUS" in light of "publicly reported information about Smartmatic's ownership and about the vulnerability of electronic voting machines to tampering." She states, "[i]t is undisputed that Smartmatic is foreign-owned and it has acquired Sequoia, one

of the three major voting machine companies doing business in the U.S.... Smartmatic's ownership is particularly troubling since Smartmatic has been associated by the press with the Venezuelan government led by Hugo Chavez, which is openly hostile to the United States."

b) On December 6, 2019, Senators Elizabeth Warren, Ron Wyden and Amy Klobuchar, and Representative Mark Pocan sent letters to Michael McCarthy of McCarthy Group, LLC that "trouble-plagued companies owned by private equity firms and responsible for manufacturing and maintaining voting machines and other election administration equipment have long skimped on security in favor of convenience, leaving voting systems across the country prone to security problems" (internal quotations omitted). The Senators and Congressman articulated concerns about the "highly concentrated" election technology industry, "with a handful of consolidated vendors controlling the vast majority of the market." They explained, "[t]oday, three large vendors – ES&S, Dominon Voting Systems, and Hart InterCivic – collectively provide voting machines and software that facilitate voting for over 90% of all eligible voters in the United States." Citing outdated machines and software that is vulnerable to hackers, they noted that "[e]lection security experts have noted for years that our nation's election systems and infrastructure are under serious threat." Finally, before asking a series of questions, the Senators and Representative detailed a sampling of problems identified during the 2018 election, including specifically that, "voters in South Carolina were reporting machines that switched their votes after they'd inputted them, scanners were rejecting paper ballots in Missouri, and busted machines were causing long lines in Indiana" (internal citations omitted). "In addition," they say, "researchers recently uncovered previously undisclosed vulnerabilities in 'nearly a dozen backend election systems in 10 states." They also cite a 2019 incident in Pennsylvania involving a state judicial election, where "the Democratic candidate's electronic tally showed that he received an improbable 164 votes out of 55,000 cast" and the county's Republican Chairwoman acknowledged that "everything went wrong" on Election Day. "These problems threaten the integrity of our elections and demonstrate the importance of election systems that are strong, durable, and not vulnerable to attack," they added.

- c) Also on December 6, 2019, Senators Elizabeth Warren, Ron Wyden and Amy Klobuchar, and Representative Mark Pocan sent a similar letter, to Stephen D. Owens and Hootan Yaghoobzadeh of Staple Street Capital Group, LLC based on reports that "Staple Street owns or has had investments in Dominion".
- 7) Multiple foreign actors have interfered in voting process of American citizens and the elections held by the United States in October and November 2020.
 - a) On October 30, 2020, the FBI and the Department of Homeland Security issued a determination and advisory that **Iran** and **Russia** had obtained and

apparently used email addresses from state voter registration lists, which include party affiliation and home addresses and can include phone numbers.

- i) It appears that those addresses were then used in a widespread targeted spamming operation. The senders claimed they would know which candidate the recipient was voting for in the Nov. 3 election, for which early voting was ongoing at the time this violation was discovered and notice was issued. Federal officials have long warned about the possibility of this type of operation, as such registration lists are not difficult to obtain.
- ii) On October 20, 2020, Christopher Krebs, then the top election security official at the Department of Homeland Security, had tweeted, "These emails are meant to intimidate and undermine American voters' confidence in our elections." This comment clearly falls within the definition of "foreign interference" under E.O. 13848 of September 12, 2018 as, "any covert, fraudulent, deceptive, or unlawful actions or attempted actions of a foreign government, or of any person acting as an agent of or on behalf of a foreign government".
- b) On October 22, 2020, CISA and the FBI issued Alert AA20-296B warning, "Iranian actors are likely intent on influencing and interfering with the US elections to sow discord among voters and undermine public confidence in the US electoral process." The alert further stated that Iranian actors are, "creating fictitious media sites and spoofing legitimate media sites to spread

- obtained US voter-registration data, anti-American propaganda, and misinformation about voter suppression, voter fraud, and ballot fraud."
- c) On October 30, 2020, CISA and the FBI issued joint Alert (AA20-304A) Iranian Advanced Persistent Threat Actor Identified Obtaining Voter Registration Data stating that "evaluation by CISA and the FBI has identified the targeting of U.S. state election websites was an intentional effort to influence and interfere with the 2020 U.S. presidential election". In addition, they wrote, "CISA and the FBI are aware of an Iranian advanced persistent threat (APT) actor targeting U.S. state websites—to include election websites. CISA and the FBI assess this actor is responsible for the mass dissemination of voter intimidation emails to U.S. citizens and the dissemination of U.S. election-related disinformation in mid-October 2020. (See FBI FLASH message ME-000138-TT, disseminated October 29, 2020).
 - i) Further evaluation by CISA and the FBI has identified the targeting of U.S. state election websites was an intentional effort to influence and interfere with the 2020 U.S. presidential election." (emphasis added).
 - ii) This finding of CISA and the FBI of this "intentional effort to influence and interfere with the 2020 U.S. presidential election" by an Iranian advanced persistent threat actor constitutes foreign interference, as defined by E.O. 13848.
- d) During the time of election night and the following morning, hundreds of thousands of fraudulent votes entered the U.S. Election system. They did so

in amounts, times, and sequences that mathematical and statistical experts have attested are a mathematical impossibility.

- 8) Just three weeks prior to the election of November 3, 2020, federal Judge Amy Totenberg found Dominion Voting Systems full of risks by "stealth vote alteration or operational interference risks posed by malware that can be effectively invisible to detection."
 - a) Judge Totenberg heard three days of testimony, including from Dominion executive Eric Coomer. The judge wrote that there are, "true risks posed by the new BMD [Ballot Marking Device of Georgia's Dominion Voting Systems] voting system as well as its manner of implementation. These risks are neither hypothetical nor remote under the current circumstances."
 - b) Continuing, she noted "the insularity of the Defendants' and Dominion's stance here in evaluation and management of the security and vulnerability of the BMD system does not benefit the public or citizens' confident exercise of the franchise." The voter does not see his actual ballot. "The printed ballot is fed into an ImageCast optical scanner that tabulates the ballot votes solely based on the QR code and not based on the human readable text on the printed ballot."
 - c) Judge Totenberg was very concerned. She stated: "The stealth vote alteration or operational interference risks posed by malware that can be effectively invisible to detection, whether intentionally seeded or not, are high once implanted, if equipment and software systems are not properly protected,

implemented, and audited. The modality of the BMD systems' capacity to deprive voters of their cast votes without burden, long wait times, and insecurity regarding how their votes are actually cast and recorded in the unverified QR code makes the potential constitutional deprivation less transparently visible as well, at least until any portions of the system implode because of system breach, breakdown, or crashes. Any operational shortcuts now in setting up or running election equipment or software creates other risks that can adversely impact the voting process."

d) Further, Judge Totenberg wrote: "The Plaintiffs' national cybersecurity experts convincingly present evidence that this is not a question of 'might this actually ever happen?' – but 'when it will happen,' especially if further protective measures are not taken. Given the masking nature of malware and the current systems described here, if the State and Dominion simply stand by and say, 'we have never seen it,' the future does not bode well. Still, this is year one for Georgia in implementation of this new BMD system as the first state in the nation to embrace statewide implementation of this QR barcode-based BMD system for its entire population. Electoral dysfunction – cyber or otherwise – should not be desired as a mode of proof. It may well land unfortunately on the State's doorstep. The Court certainly hopes not."²

² Case 1:17-cv-02989-AT Document 964 Filed 10/11/20 Page 146 of 147.

- 9) Every defect and hazard of which Judge Totenberg warned happened in Georgia and across the country.
 - a) Witnesses in Georgia, Arizona, Michigan, Wisconsin, Pennsylvania, and other states, have attested to election computer crashes, replacements of a server, impermissible and untested updates to the system, and connections to the internet—among countless other election law violations and irregularities.
 - b) Both Coffee and Ware counties in Georgia have identified a significant percentage of votes being wrongly allocated, contrary to the will of the voter. Ware County, Georgia, upon a full hand recount of its ballots, found a 37 vote discrepancy between the electronic tabulation of the vote and the hand recount, identifying a vote flip of 37 votes from President Trump to Biden. Extrapolated over the counties of Georgia corresponds to a more than 56,000 vote difference.
 - c) Coffee County, Georgia Board of Elections had to refuse to certify its vote because during the November 30, 2020 recount, the Dominion Voting Systems produced 39 new votes for President Trump without any change in total ballots cast. In this same recount, the Board scanned 185 missing recount ballots into the results, yet the Dominion tabulator found no change in the votes for any candidate. On December 2, 2020, during Georgia's third recount, the same original results were produced, ignoring the 185 new ballots.
 - d) Analysis has established that there was a 5.6 % increase in votes for one candidate for president across the entire Dominion system—with all other variables frozen.

Exhibit 83

TIMELINE Foreign Interference in the 2020 U.S. Election

- October 6, 2006 Congressman Maloney Letter: On October 6, 2006, citing concerns about foreign influence and control over Dominion machines and Smartmatic/Sequoia software, Representative Carolyn B. Maloney sent a letter to the then-Secretary of the Treasury, Henry M. Paulson, Jr. "seeking review by the Committee on Foreign Investment in the United States of the acquisition of Sequoia Voting Systems by Smartmatic, a foreign-owned company."
 - o December 6, 2019 Senators Elizabeth Warren, Ron Wyden, Amy Klobuchar, and Representative Mark Pocan sent a similar letter to Stephen D. Owens and Hootan Yaghoobzadeh of Staple Street Capital Group, LLC based on reports that Staple Street owns or has had investments in Dominion.
- January, 2017 DHS designated election infrastructure used in federal elections as "critical infrastructure."
- September 12, 2018 The President issued E.O. 13848, declaring a National Emergency, to address the threat of foreign interference in U.S. elections based on the ability of foreign actors to interfere in and undermine public confidence in elections.
 - o The term "foreign interference," with respect to an election, includes any covert, fraudulent, deceptive, or unlawful actions or attempted actions of a foreign government, or of any person acting as an agent of or on behalf of a foreign government, undertaken with the purpose or effect of influencing, undermining confidence in, or altering the result or reported result of, the election, or undermining public confidence in election processes or institutions.
- August 18, 2020 Bipartisan Senate Intelligence Committee report warned of known vulnerabilities of major voting systems used throughout the country and the likelihood of fraud and hacking in the upcoming elections.
 - The Report describes penetration by Russian cyber actors, including the Illinois voter registration database in 2018.
 - The Committee identified evidence of common software, which is in voting machines used by over 90% of voters across the country.
 - The Committee heard testimony about the ability of operators to "reprogram" the machine to invisibly cause any candidate to win."
- October, 2020 The FBI and CISA issued 2 Alerts about Iranian interference in the U.S. 2020 election.

- The FBI and CISA "are aware of an Iranian advanced persistent threat (APT) actor targeting U.S. state websites – to include election websites. CISA and the FBI assess this actor is responsible for the mass dissemination of voter intimidation emails to U.S. citizens and the dissemination of U.S. election related disinformation in mid-October 2020."
- o FBI and CISA also observed:
 - Targeting of U.S. state election websites in an "intentional effort to influence and interfere with the 2020 U.S. presidential election";
 - Exploitation of multiple legacy vulnerabilities directed at federal, state, local, tribal and territorial government networks.
 - Activity resulting in unauthorized access to election support systems;
- On and around November 3, 2020 Experts and governments witnessed attacks on U.S. critical election infrastructure.
 - Attacks were designed to undermine the integrity and reliability of American elections, and specifically to flip the election to Presidential candidate Joseph Biden.
 - Experts examined the various companies, networks, structures, machines and related global infrastructure directly tied to the 2020 US Election and found clear foreign interference.
 - December 2020 Retired senior military officer stated, "This assessment contains clear and definitive evidence that foreign interference...occurred prior to, and during, the General Election."
 - o The Nevada Secretary of State sent personally identifiable information of voters to a tech firm based in Pakistan, with ties to Pakistan intelligence agency.
 - Electronic information from US elections went to Germany, Barcelona, Serbia and Canada
 - Dominion servers in Belgrade, Serbia; Toronto, Canada
 - o Scytl in Frankfurt, Germany; Barcelona, Spain; and Ireland
- Affidavit of Venezuelan Whistleblower Former senior military officer and direct aide to Hugo Chavez gave a sworn statement that Dominion was designed to enable vote manipulation and used to keep Hugo Chavez in power.
- On December 18, 2020 Treasury Department issued sanctions on a Venezuelan company and individuals in relation to the Maduro regime's efforts to steal elections in Venezuela.

Exhibit 84

Case 1:21-cv-00040 Document 1-83 Filed 01/08/21 Page 2 of 2

screenshot-twitter.com-2021.01.06-14_11_22 https://twitter.com/SidneyPowell1/status/1345679327887843329?s=20 06.01.2021



Exhibit 85

2020 ELECTION EVIDENCE OF FOREIGN INTERFERENCE

SIDNEY POWELL

AUTHOR OF THE BESTSELLER LICENSED TO LIE

About
Court Filings / Evidence
News SCOTUS Shop

'n,

Search

2020 Election Evidence Summary

Summary Evidence Election 2020 by Sidney Powell on Scribd



Fighting to expose the truth.

Contact

2020 Election Evidence Summary

Summary Evidence Election 2020 by Sidney Powell on Scribd



Fighting to expose the truth.

Privacy Policy | Terms & Conditions

Copyright © 2021 Sidney Powell

Contact
Invite To Speak
Support
Shipping &
Returns

Exhibit 86

SCOTUS FILINGS HERE: ARIZONA GEORGIA MICHIGAN WISCONSIN

SIDNEY POWELL

SCOTUS

News Shop

Search



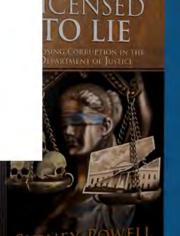
DONATE TO DEFEND THE REPUBLIC!!

Defending the Republic was established by Sidney Powell to defend and protect the integrity of elections in the United States.

DONATE HERE

NSJ Nonfiction eBook t Seller in Professional Law Ethics, US Judicial White Collar Crime

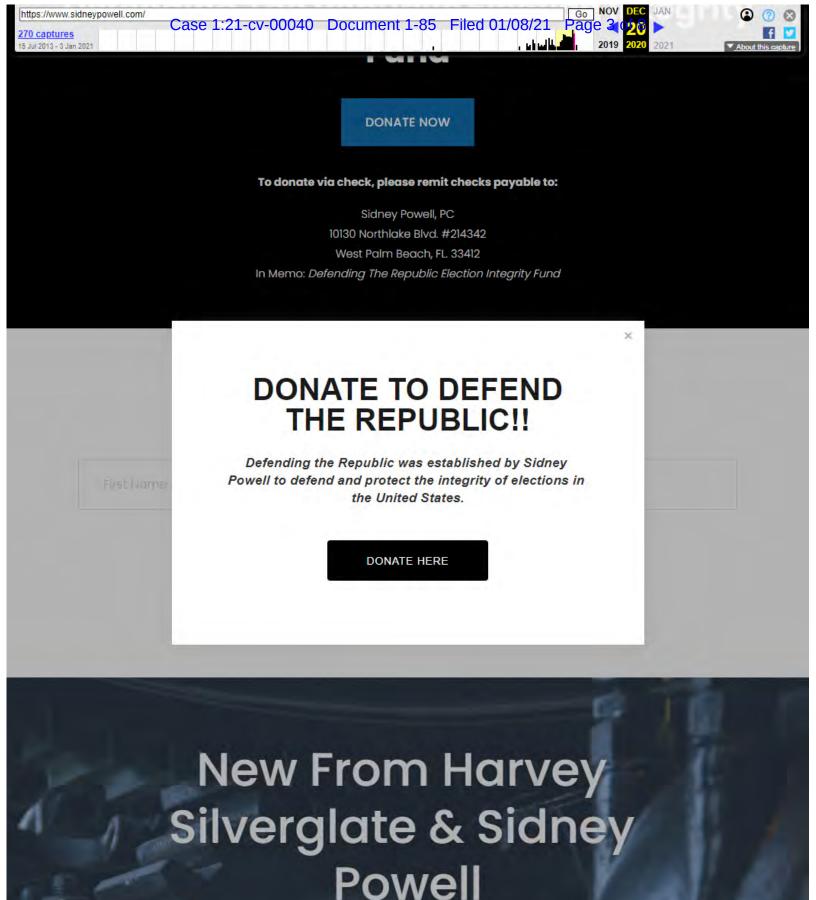
*5 National Best Seller

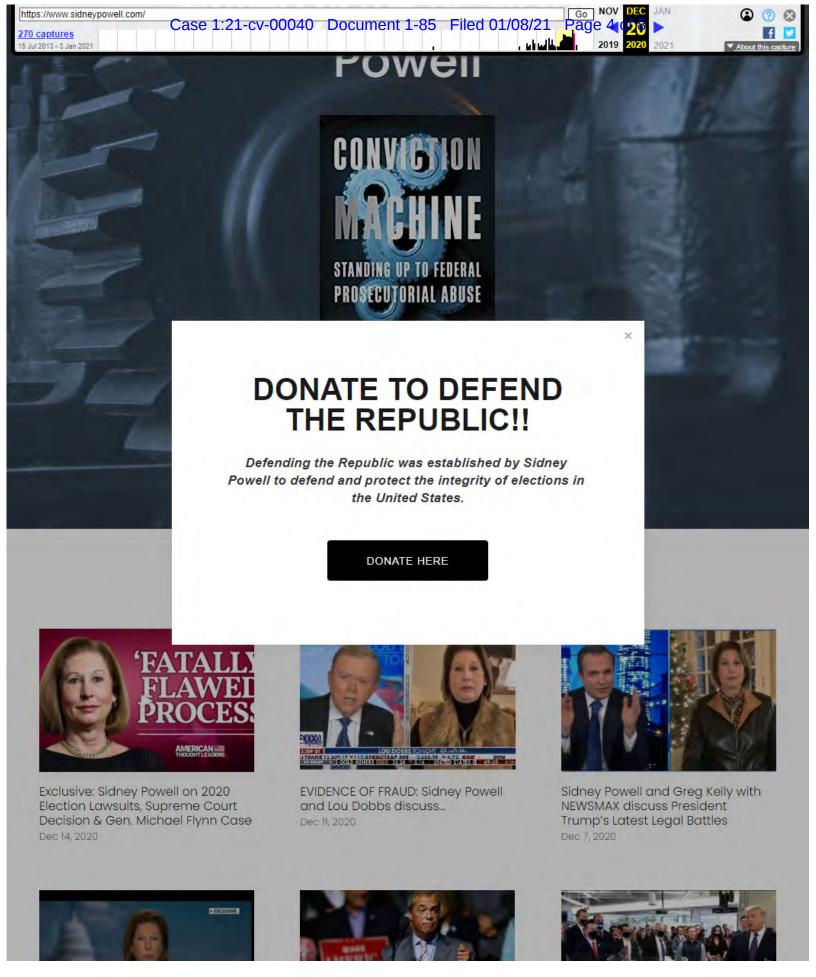


Defending The Republic Election Integrity Fund

DONATE NOW

Page 1 of 7





Page 3 of 7

270 captures

Nancy Pelosi's Chief of Staff Is Chief Executive and Feinstein's Husband a Shareholder at Dominion Nov 8, 2020



Farage Urges Trump to 'Keep Up the Fight', Highlights Fraud in UK Postal Voting Nov 7, 2020



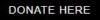
Sidney Powell: Trump has to fight for election integrity Nov 6, 2020



Sidney Powell, Tom Fitt Dobbs discuss #Hamr #Scorecard Nov 8, 2020

DONATE TO DEFEND THE REPUBLIC!!

Defending the Republic was established by Sidney Powell to defend and protect the integrity of elections in the United States.





endorses Doug rgia Senate race

What People Are Saying

"It would be malpractice to litigate against the Department of Justice without reading this book."

"That our government is corrupt is the only conclusion. This book helps the people understand the nature of this

270 captures



it would be malpractice to litigate

against the Department of Justice without reading this book."

-- Brendan Sullivan Jr. | Williams & Connolly LLP

"This book reads like a cross between investigative journalism and courtroom drama."

 – Jane Davis | Former lead prosecutor, District Courts, Bexar County, Texas

only conclusion. This book helps the people understand the nature of this corruption—and how it is possible for federal prosecutors to indict and convict the innocent rather than the guilty. Every business person- and anyone- who values freedom should read and heed the warnings of this compelling work."

"This book shou of a serious con our criminal just

live up to its vau citizens of a free

important stake

does."

Alex Kozinski

DONATE TO DEFEND THE REPUBLIC!!

Defending the Republic was established by Sidney Powell to defend and protect the integrity of elections in the United States.

DONATE HERE

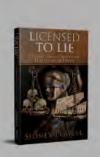
ling this fastto stand up age in daring est recesses of he only ax

andeo | CEO & Author

or of The Yellow House

Shop

Due to increasing demand, new book orders are on backorder until January 1, 2021













LICENSED TO LIE: Exposing Corruption in the Department of Justice (Second Edition) \$40.00

LICENSED TO LIE: Exposing Corruption in the Department of Justice (Autographed Second Edition) \$60.00

LICENSED TO LIE: Exposing Corruption in the Department of Justice (Autographed Second Edition w/ Personal Message) \$100.00

LICENSED TO LIE: **Exposing Corruption in** the Department of Justice (Second Edition Paperback)

\$20.00

"Creeps On A Mission" T-Shirt from \$25.00



Fighting to expose the truth.

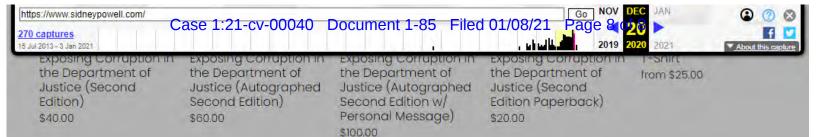
Privacy Policy | Terms & Conditions

WINNER

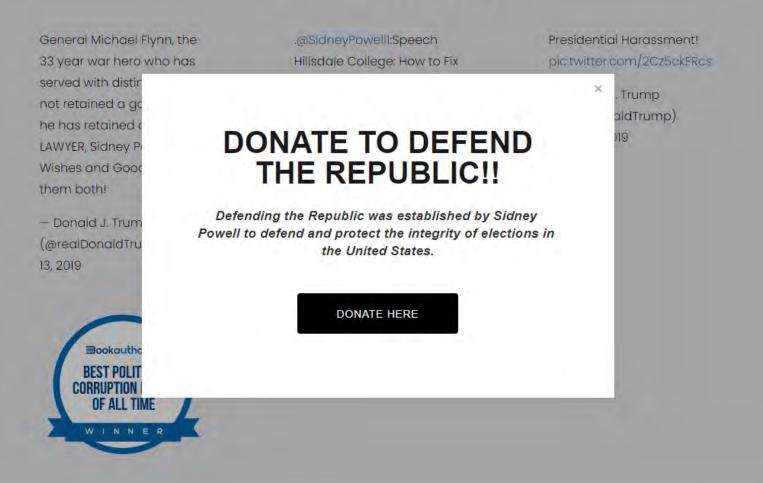
Contact

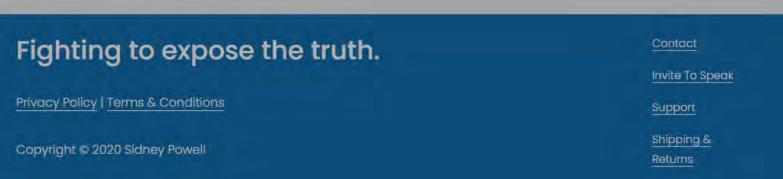
Invite To Speak

Support



Endorsements





Document title: (Signey Pry211-Ayboo 1919 Best CLICENS) to Discument 22-7 Filed 01/20/22 Page 326 of 591 PageID

Capture URL: https://web.archive.org/web/20201220235533/https://www.sidneypgwell@and

Exhibit 87

70 captures



SCOTUS FILINGS HERE: ARIZONA GEORGIA MICHIGAN WISCONSIN

SIDNEY POWELL AUTHOR OF THE BESTSELLER LICENSED TO LIE

SCOTUS

Shop

Search

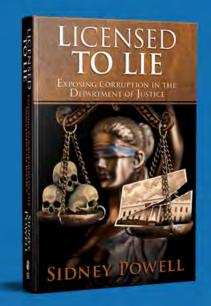


Federal Appeals Creeps On A Mission Licensed To Lie

#5 National Best Seller

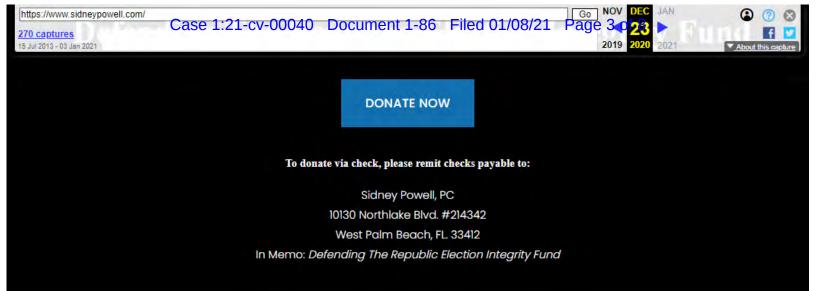
#1 Best Seller WSJ Nonfiction eBook

#1 Amazon Best Seller in Professional Responsibility & Law Ethics, US Judicial Branch, and White Collar Crime



Defending The Republic Election Integrity Fund

DONATE NOW

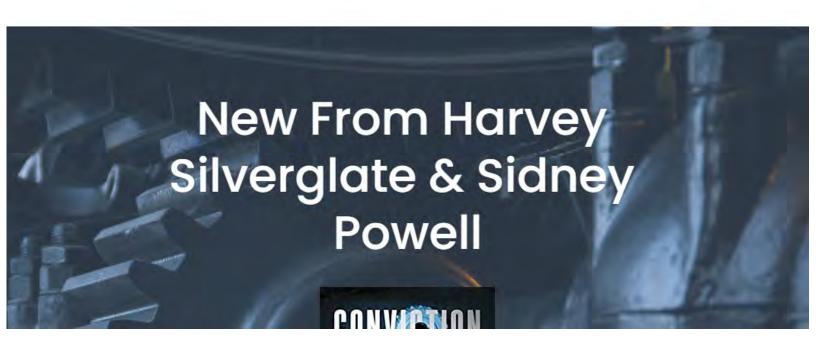


Newsletter Sign-up

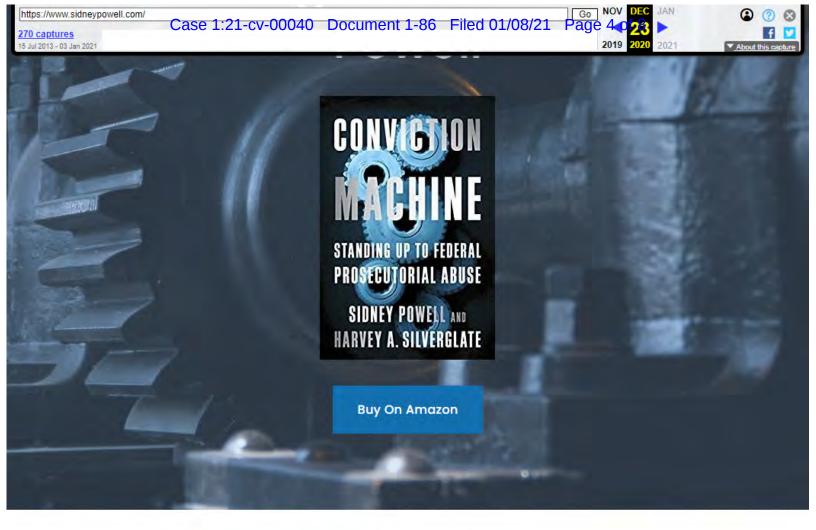
Sign up with your email address to receive news and updates.

Sign Up

We respect your privacy.



Page 2 of 7



In The Media



Exclusive: Sidney Powell on 2020 Election Lawsuits, Supreme Court Decision & Gen. Michael Flynn Case Dec 14, 2020



EVIDENCE OF FRAUD: Sidney Powell and Lou Dobbs discuss... Dec 11, 2020



Sidney Powell and Greg Kelly with **NEWSMAX** discuss President Trump's Latest Legal Battles Dec 7, 2020





270 captures



Nancy Pelosi's Chief of Staff Is Chief Farage Urges Trump to 'Keep Up the Fight', Highlights Fraud in UK Postal Voting

Nov 7, 2020



Sidney Powell: Trump has to fight for election integrity Nov 6, 2020



Executive and Feinstein's Husband

a Shareholder at Dominion

Nov 8, 2020

Nov 6, 2020

Sidney Powell, Tom Fitton, Lou Dobbs discuss #Hammer & #Scorecard

SIDNEY POWELL: DEMS WILL USE 'LAWFARE' TO ALTER ELECTION

Sidney Powell: Dems Will Use 'Lawfare' To Alter Election Nov 5, 2020



Michael Flynn endorses Doug Collins in Georgia Senate race Oct 20, 2020

View More

What People Are Saying

"It would be malpractice to litigate against the Department of Justice without reading this book."

Brendan Sullivan Jr. | Williams & Connolly LLP

"That our government is corrupt is the only conclusion. This book helps the people understand the nature of this corruption—and how it is possible for

against the Department of Justice without reading this book."

- Brendan Sullivan Jr. | Williams & Connolly LLP

"This book reads like a cross between investigative journalism and courtroom drama."

> — Jane Davis | Former lead prosecutor, District Courts, Bexar County, Texas

only conclusion. This book helps the people understand the nature of this corruption—and how it is possible for federal prosecutors to indict and convict the innocent rather than the guilty. Every business person- and anyone- who values freedom should read and heed the warnings of this compelling work."

- Victor Sperandeo | CEO & Author

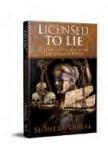
"This book should serve as the beginning of a serious conversation about whether our criminal justice system continues to live up to its vaunted reputation. As citizens of a free society, we all have an important stake in making sure that it does."

- Alex Kozinski | Chief Judge, United States Court of Appeals for the Ninth Circuit "When you've finished reading this fastpaced thriller, you will want to stand up and applaud Powell's courage in daring to shine light into the darkest recesses of America's justice system. The only ax Powell grinds here is Truth."

- Patricia Falvey | Author of The Yellow House

Shop

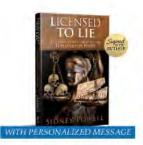
Due to increasing demand, new book orders are on backorder until January 1, 2021



LICENSED TO LIE:



LICENSED TO LIE:



LICENSED TO LIE:



LICENSED TO LIE:



"Creeps On A Mission"

Page 5 of 7

270 captures







LICENSED TO LIE: Exposing Corruption in the Department of Justice (Second Edition) \$40.00



LICENSED TO LIE: Exposing Corruption in the Department of Justice (Autographed Second Edition) \$60.00



LICENSED TO LIE: Exposing Corruption in the Department of Justice (Autographed Second Edition w Personal Message) \$100.00



Page 70

LICENSED TO LIE: Exposing Corruption in the Department of Justice (Second Edition Paperback) \$20.00



"Creeps On A Mission" T-Shirt from \$25.00

Endorsements

General Michael Flynn, the 33 year war hero who has served with distinction, has not retained a good lawyer, he has retained a GREAT LAWYER, Sidney Powell. Best Wishes and Good Luck to them both!

- Donald J. Trump (@realDonaldTrump) June 13, 2019



.@SidneyPowell1:Speech Hillsdale College: How to Fix Justice! Discusses @GenFlynn case as well as Enron case, 5% of prison population probably not guilty, another 5% had inadequate counsel. Withholding Brady Material needs severe sanctions!https://t.co/6Yxe

- Ken Jones☆☆☆ (@sxdoc) March 11, 2020

n5x990

Presidential Harassment! pic.twitter.com/2Cz5ckERcs

- Donald J. Trump (@realDonaldTrump) March 5, 2019

Fighting to expose the truth.

Privacy Policy | Terms & Conditions

Contact

Invite To Speak

Support

270 captures





exposing corruption the Department of Justice (Second Edition) \$40.00

exposing corruption if the Department of Justice (Autographed Second Edition) \$60.00

exposing contaption in the Department of Justice (Autographed Second Edition w/ Personal Message) \$100.00

exposing contablion the Department of Justice (Second Edition Paperback) \$20.00

from \$25.00

Endorsements

General Michael Flynn, the 33 year war hero who has served with distinction, has not retained a good lawyer, he has retained a GREAT LAWYER, Sidney Powell. Best Wishes and Good Luck to them both!

- Donald J. Trump (@realDonaldTrump) June 13, 2019



.@SidneyPowell1:Speech Hillsdale College: How to Fix Justice! Discusses @GenFlynn case as well as Enron case, 5% of prison population probably not guilty, another 5% had inadequate counsel. Withholding Brady Material needs severe sanctions!https://t.co/6Yxe n5x990

– Ken Jones☆☆☆☆ (@sxdoc) March 11, 2020 Presidential Harassment! pic.twitter.com/2Cz5ckERcs

 Donald J. Trump (@realDonaldTrump) March 5, 2019

Fighting to expose the truth.

Privacy Policy | Terms & Conditions

Copyright © 2020 Sidney Powell

Contact

Invite To Speak

Support

Shipping & Returns







Exhibit 88





Sidney Powell.

Since the 2020 election, Sidney Powell has put together a small and dedicated team of Patriots to uncover and begin litigating the massive election fraud the country just experienced especially but not exclusively through the Dominion voting machines.

Defending the Republic was created to help fund this enormously important litigation and to pursue any other litigation that might be needed to keep this extraordinary Republic and "secure the blessings of liberty for ourselves and our posterity."

33 captures



needed to keep this extraordinary Republic and "secure the blessings of liberty for ourselves and our posterity."

To contact Sidney Powell directly, please visit her website: https://www.sidneypowell.com

Millions of dollars must be raised to defend the Republic as these lawsuits continue to be filed to ensure victory.

In Bush v. Gore the Supreme Court recognized that once vested in the people, the right to vote is fundamental, and one source of its fundamental nature lies in the equal weight of each vote.

This fundamental right to equal weight was not defended or actualized in this election. There is evidence of ballots being discarded, hundreds of thousands of ballots appearing out of thin air, ballot harvesting, and a lower standard of verification for some mail-in ballots. This is voter fraud and has infringed upon Americans sacred right to vote and for their votes to carry equal weight.

The case will seek to block the certification of the election results so that justice can be done. We need to stop the steal in its tracks.

The future of our Republic is at stake. The left, the media, and a complicit Republican Establishment are attempting to steal this election through a staggering voter fraud operation. The time to fight is now!

THE KRAKEN IS

Contribute to Defend the Republica



THE KRAKEN IS RELEASED

"The right to do what the law does not prohibit, without fear of harassment or punishment, is one of the hallmarks of a free society." - Sidney Powell

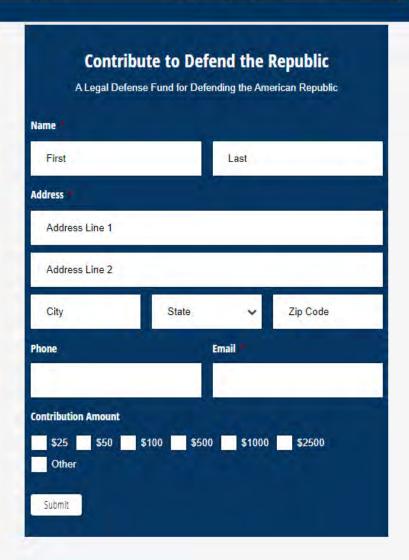
Since Defending the Republic was established by Sidney Powell to defend and to protect the integrity of elections in the United States. Please contribute below, using our secure system. Your donation will support our mission and the welfare of the American Republic.

Please make any/all checks payable to: Defending the Republic LLC

Sidney Powell, P.C.

10130 Northlake Blvd, #214342 West Palm Beach, Florida 33412

Memo: Defending The Republic Election Integrity



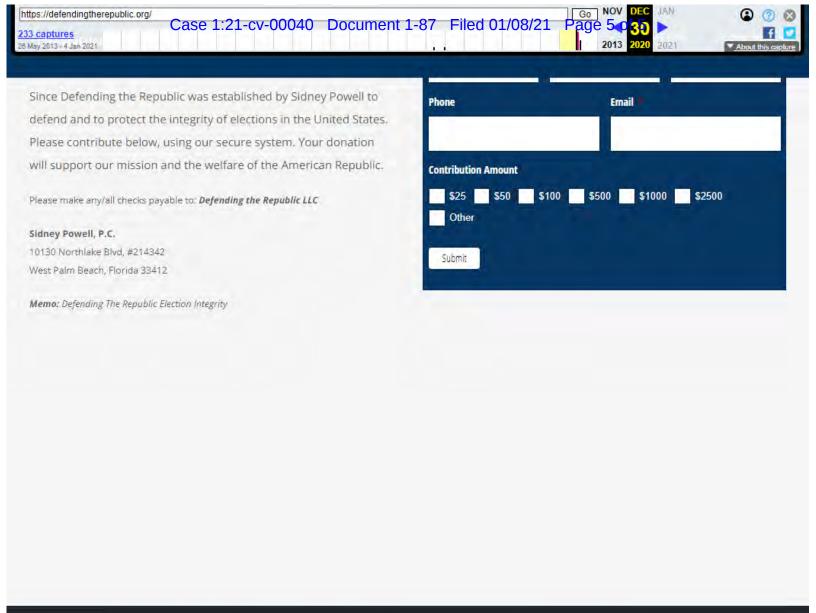
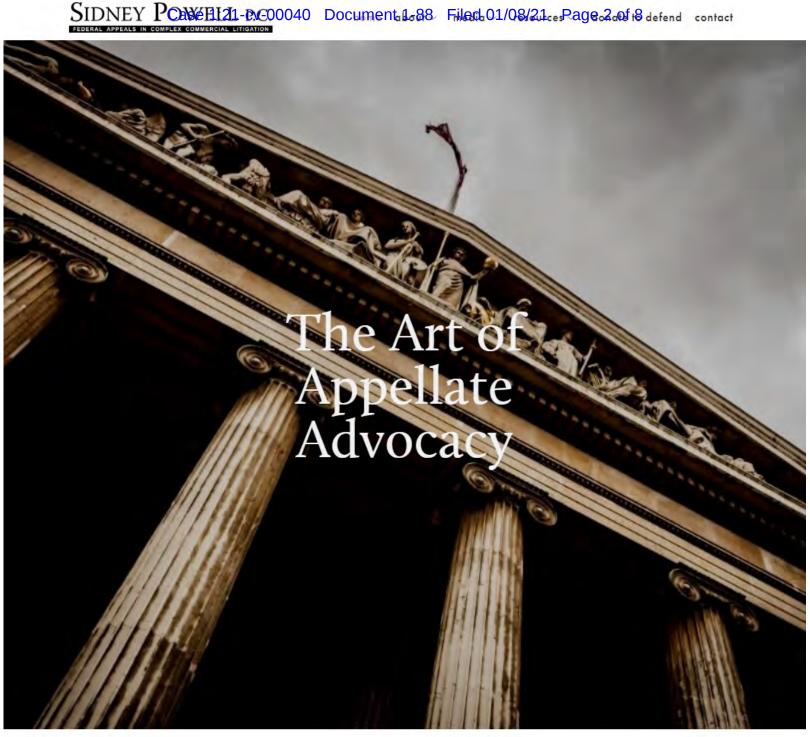


Exhibit 89



500+

180+

90+%

70+%

CASES AS LEAD COUNSEL

PUBLISHED OPINIONS

SUCCESSFUL AFFIRMANCE

SUCCESSFUL CASE REVERSAL RATE

Areas of Practice

Areas of Practice



White Collar Criminal Defense

Financially motivated, nonviolent crime committed by business and government professionals. Typical white-collar crimes could include fraud, bribery, Ponzi schemes, insider trading, labor racketeering, embezzlement, cybercrime, copyright infringement, money laundering, identity theft, and forgery.



Commercial Litigation

Commercial litigation encompasses disputes and litigation which go to the core of a company's business strategy and business implementation.



Patent, Trademark, Copyright, and Intellectual Property

A wide body of federal and state laws protects creative property such as writing, music, drawings, paintings, photography, and films.



National Defense Contract and Technology

Given today's globalized access to knowledge and the rapid pace of technology development, innovation, speed, and agility have taken on a greater importance.

Sidney Powell P.C.

Sidney Powell practices the art of appellate advocacy.

More and more, experienced trial and corporate counsel recognize the difference in skills needed to successfully represent clients on appeal and the advantage that an experienced federal appellate lawyer adds to the trial team. Whether the client seeks to affirm a large existing verdict or reverse an adverse result, retaining Sidney Powell P.C. will maximize chances of success.

Sidney Powell's appellate experience is unparalleled. She has been lead counsel in more than 500 federal appeals resulting in more than 180 published opinions. Careful parsing of the record, thorough research, and persuasive legal writing are the hallmarks of the briefs filed by Sidney Powell, P.C.

The firm accepts only a few selected cases each year and gives each the personal time and attention it deserves. We craft our briefs to present each client's case in the most persuasive, well-documented, and professional format possible. Our clients include lawyers, judges, prominent individuals, cities, counties, and international corporations.

LEARN MORE

Page 2 of 7

The firm accepts only a few selected cases each byear and gives each the personal time and attention it deserves. We craft our briefs to present each client's case in the most persuasive, well-documented, and professional format possible. Our clients include lawyers, judges, prominent individuals, cities, counties, and international corporations.

LEARN MORE

Significant Reversals

Although statistically the Fifth Circuit reverses only **approximately 15**% of its cases, Sidney Powell has succeeded in reversing **more than 70**% of the cases in which she has represented the appellant and sought reversal. Some of our most significant reversals for our clients include:

2018

IAS SERVICES GROUP LLC V. JIM BUCKLEY & ASSOCIATES INC. ET AL. (5TH CIR. 2018)

Reversing multi-million dollar judgment in its entirety and obtaining reinstatement of a wrongly dismissed fraud claim.

2015

TRANSVERSE, L.L.C. V. IOWA WIRELESS SERVICES, L.L.C., 617 F. APP'X 272 (5TH CIR. 2015)

Reversed and vacated \$13 million damages award.

2014

WILLIAMS-BOLDWARE V. DENTON CO., TEX., 741 F.3D 635 (5TH CIR. 2014)

Reversing a Title VII racially hostile workplace environment claim against the County which had acted promptly and positively to solve any problem. The title VII judgement and award was reversed and rendered for the client.

2008

KADLEC MEDICAL CENTER V. LAKEVIEW ANESTHESIA ASSOCIATES, 527 F.3D 412 (5TH CIR. 2008)

Reversing \$8 million judgment against a hospital.

2006

US V. BROWN (5TH CIR. 2006)

We obtained the reversal of the conspiracy and fraud convictions

2003

AMERICAN REALTY TRUST V. MATISSE PARTNERS, NO. 03-10462, (5TH CIR. 2003).

We obtained the reversal of a district court's dismissal of a complex case involving issues of pre-emption, removal and remand, artful pleading and federal jurisdiction.

2000

WASTE CONTROL SERVICES, INC: 199 F.3D 781 (5TH CIR. 2000)

We obtained the reversal of a multi-million dollar judgment that had been wrongly entered by the district court against American Realty Trust in a case involving breach of contract and fiduciary duties arising out of a consulting contract between this national real estate investment company and its consultants, Matisse Partners. The Fifth Circuit reinstated the jury's findings that Matisse Partners had breached its contract with American Realty and had breached its fiduciary duties to the company.

MUSSER DAVIS LAND COMPANIES: 201 F.3D 561, 145 OIL & GAS REP. 282 (5TH CIR. 2000)

Sidney Powell was lead counsel for Union Pacific Resources and succeeded in obtaining a reversal of the district court's decision which had adversely affected the ability of oil companies to perform seismic testing in Louisiana.

1998

AT&T: 154 F.3D 226 (5TH CIR 1998)

Sidney Powell was co-counsel on the AT&T team which

2006

US V. BROWN (5TH CIR. 2006)

We obtained the reversal of the conspiracy and fraud convictions of Merrill Lynch executives.

HODGES V. MACK TRUCKS

Reversing \$8 million judgment against Mack Trucks in a product liability action.

1998

AT&T: 154 F.3D 226 (5TH CIR 1998)

Sidney Powell was co-counsel on the AT&T team which succeeded in obtaining a reversal of the district court's declaration that a section of the Federal Telecommunications Act was unconstitutional.

Clients







lowa Wireless Services, LLC



Hospital
Corporation of
America

Arthur Anderson

Denton County, Texas Iowa Wireless Services, LLC TriMax Media

Testimonials

"A brilliant lawyer; a fearless advocate who puts her heart in her work. She immediately identified the winning issues and fought tirelessly on my behalf."

"She has a passion for her work. Probably the leading 5th Circuit practitioner in Texas. She has a passion for her work."

TEXAS LAWYER'S GO-TO GUIDE

- JIM BROWN

her work. She immediately practitioner in Texas. She has a Case 1:21-cv-00040 Document 1-88 Filed 01/08/21 Page 6 of 8 identified the winning issues and passion for her work." fought tirelessly on my behalf."

TEXAS LAWYER'S GO.TO GUIDE

- JIM BROWN

"I hired Sidney Powell on two cases while I was practicing law. Both were appeals to the 5th Circuit and she won them both. She is a great writer and her appearance in the court room is even more dramatic. I give her my highest recommendation."

- KENT R. HANCE, CHANCELLOR TEXAS TECH UNIVERSITY SYSTEM

"It would be malpractice to litigate against the Department of Justice without reading this book."

- BRENDAN V. SULLIVAN, JR. WILLIAMS & CONNOLLY (IN REFERENCE TO LICENSED TO LIE)

Meet The Team





SIDNEY POWELL

President

Capture timestamp (UTC): Mon, 04 Jan 2021 15:00:45 GMT

Sidney Powell established her own firm dedicated to federal appellate practice in January

MOLLY MCCANN

Counsel

Molly McCann is Of Counsel with Sidney Powell, P.C. She is a graduate of George

President

Sidney Powell established her own firm dedicated to federal appellate practice in January 1993. She has served as lead counsel in more than 500 appeals in the Fifth Circuit, which have resulted in more than 180 published opinions.

Counsel

Molly McCann is Of Counsel with Sidney Powell, P.C. She is a graduate of George Mason University's Scalia Law School in Arlington, Virginia.

READ FULL BIO -

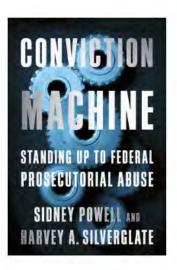
READ FULL BIO →

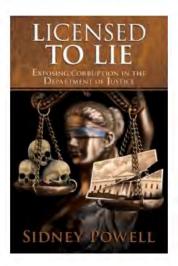


Get The Books

Conviction Machine

Prosecutors can "indict a ham sandwich," we hear, and laugh at the absurdity. Yet the joke captures a truth: federal prosecutors wield enormous power over us all. And the federal criminal justice system is so stacked in favor of the government that shocking numbers of innocent people have been sent to prison. Get the book now.





Licensed To Lie

...is the inside story of the most high-profile prosecutions of the last decade, and it's a 5-star great mystery read on Amazon. This book provides a frightening perspective on justice and who should be accountable when evidence is withheld and prosecutors break the law. Get the book now.

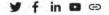
GET IN CONTACT

home about services media resources contact

Practicing primarily in the United States Court of Appeals, Sidney Powell, P.C.

шоп тоо роонапед оринова

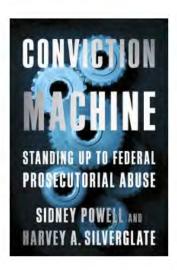
Case 1:21-cv-00040 Document 1-88 Filed 01/08/21 Page 8 of 8 READ FULL BIO -

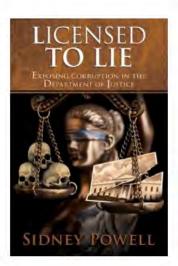


Get The Books

Conviction Machine

Prosecutors can "indict a ham sandwich," we hear, and laugh at the absurdity. Yet the joke captures a truth: federal prosecutors wield enormous power over us all. And the federal criminal justice system is so stacked in favor of the government that shocking numbers of innocent people have been sent to prison. Get the book now.





Licensed To Lie

...is the inside story of the most high-profile prosecutions of the last decade, and it's a 5-star great mystery read on Amazon. This book provides a frightening perspective on justice and who should be accountable when evidence is withheld and prosecutors break the law. Get the book now.

GET IN CONTACT

home about services media resources contact

214.707.1775 2911 Turtle Creek Blvd. #300 Dallas, TX 75219-4480

Practicing primarily in the United States Court of Appeals, Sidney Powell, P.C. represents clients in a wide variety of civil and criminal litigation in our federal courts...

Read More →

The information you obtain at this site is not, nor is it intended to be, legal advice. Please see our Disclaimer / Use of Materials. Copyright © 2021 Sidney Powell P.C.

Capture timestamp (UTC): Mon, 04 Jan 2021 15:00:45 GMT

Exhibit 90

Case 1:21-cv-00040 Document 1-89 Filed 01/08/21 Page 2 of 9 20201109 Sunday Morning futures with Maria Bartiromo November 08, 2020

File:
20201109 Sunday Morning Futures with Maria Bartiromo
Sidney Powell ELECTION FRAUD
Full Show November 8, 2020

1 MARIA BARTIROMO: -- legal team, as you've 2 been hearing this morning, are preparing for all 3 out war. 4 Beginning with a slew of new lawsuits this 5 week, beginning with one in Pennsylvania tomorrow, 6 along with what our next guest says is evidence of 7 voter fraud. 8 Sidney Powell is General Michael Flynn's 9 attorney; she is fighting on the front lines of 10 this battle, as part of the President's legal 11 team. 12 Sidney, good morning to you. Thank you for 13 being here. Can you walk us --14 SIDNEY POWELL: Good --15 MARIA BARTIROMO: -- through what has taken 16 place --17 SIDNEY POWELL: Good morning, Maria. 18 MARIA BARTIROMO: -- here as you see it. 19 SIDNEY POWELL: Yes. There has been a massive and coordinated effort to steal this 20 21 election from We the People of the United States 2.2 of America, to delegitimize and destroy votes for 23 Donald Trump, to manufacture votes for Joe Biden. 24 They have done it every way imaginable, from 25 having dead people vote in massive numbers to

1 absolutely fraudulently comp- -- creating ballots 2 that exist only voting for Biden. 3 We've identified at least 450,000 ballots 4 in the key states that miraculously only have a 5 mark for Joe Biden on them, and no other candidate. 6 If you look at Florida, where things were done right, you can see that that's how the rest 8 9 of the country should have gone; but they also 10 used an algorithm to calculate the votes they 11 would need to flip, and they used the computers to 12 flip those votes from Biden to -- I mean, from 13 Trump to Biden, and from other republican 14 candidates to their competitors also. 15 I think Doug Collins had the race stolen 16 from him. I think John James had his race stolen 17 from him. It wasn't just President Trump; there were many people affected by this. 18 19 We have got to fight tooth and nail in 20 Federal Court to expose this abject fraud and the 21 conspiracy behind it, and get a recount and audits 2.2 in every place it's needed; which is, frankly, 23 most of the country. 24 MARIA BARTIROMO: So there are recounts 25 going on right now; we know that in Georgia.

1 have a list of numbers of ballots with only Joe 2 Biden on the ticket. You saw it's 98,000 ballots 3 in Pennsylvania, 80 to 90,000 in Georgia; another 4 42,000 in Arizona. 69 to 115,000 in Michigan, and 5 62,000 in Wisconsin. Sidney, if this is true, this appears 6 7 systemic, where is the Department of Justice? 8 Where is the AG, Bill Barr? If this is so 9 obvious, then why aren't we seeing massive 10 government investigations? SIDNEY POWELL: I don't know. 11 We 12 definitely should be. I mean, we're getting 13 reports of all kinds of fraud. We've got a --14 getting a affidavit from a postal worker now who 15 talks about having been ordered to backdate 16 ballots. No ballots received after the polls 17 closed on voting day should even be counted. 18 We've got multiple states that didn't even follow 19 the rules of their own legislature. That's a federal constitutional issue. 20 21 There are at least three major federal 22 issues here that will require the Supreme Court to 23 revolve these -- this case. 24 And when the --25 MARIA BARTIROMO: Okay.

1 SIDNEY POWELL: -- the votes are really 2 audited, and the real votes are counted, Trump 3 will win. He is the president, and he is in 4 charge of this country. 5 MARIA BARTIROMO: Sidney, I want to ask you about these algorithms and the Dominion software. 6 7 I understand Nancy Pelosi has an interest in this 8 company. 9 Let's take a break; we'll come back with 10 that. 11 I'm talking with Sidney Powell this morning 12 on her legal strategy. Stay with us. 13 Welcome back. I'm back with Sidney Powell, 14 who is part of President Trump's legal team in 15 contesting this election. 16 Sidney, we talked about the Dominion 17 software. I know that there were voting 18 irregularities. Tell me about that. 19 SIDNEY POWELL: That's putting it mildly. 20 The computer glitches could not and should not have happened in -- at -- at all. 21 2.2 Those -- that is where the fraud took place 23 where they were flipping votes in the computer 24 system, or adding votes that did not exist. 25 We need an audit of all the computer

1 systems that were -- played any role in this fraud 2 whatsoever. 3 And, you know, Joe Biden had it right; he 4 said that he had the biggest voter fraud 5 organization ever, and he didn't need people's 6 votes now, he would need people later. They had this all planned, Maria. They had 8 the algorithms. They had the paper ballots 9 waiting to be inserted if and when needed. 10 And notably, President Trump's vote in the 11 blue states went up enormously. That's when they 12 had to stop the vote count and go in and replace 13 votes for Biden and takeaway Trump votes. 14 MARIA BARTIROMO: I never seen voting 15 machines stop in the middle of an election. 16 Stopped, downed and assessed the situation. 17 I also see reports that Nancy Pelosi's 18 longtime chief of staff is a key executive at that 19 company; Richard Blum, Senator Feinstein's husband, a significant shareholder of the company. 20 21 What can you tell us about the interest on 2.2 the other side of this Dominion software? 23 SIDNEY POWELL: Well, obviously, they have 24 invested in it for their own reasons, and are 25 using it to commit this fraud to steal votes.

1 I think they've even stolen them from other democrats in their own party who should be 2 3 outraged about this also. 4 Bernie Sanders --5 MARIA BARTIROMO: Wow. SIDNEY POWELL: -- might very well have been 6 7 the democratic candidate, but they've stolen 8 against whoever they wanted to steal it from. 9 MARIA BARTIROMO: Sidney, these are 10 incredible charges that you are making this 11 morning. We, of course, will be following this. 12 And we thank you for joining me today. Please 13 come back soon. 14 Sidney Powell. That will do it for 15 Sunday --16 (End of the recording.) 17 18 19 20 21 2.2 23 24 25

1	CERTIFICATE
2	
3	I, JACKIE MENTECKY, do hereby certify that
4	I was authorized to transcribe the foregoing recorded
5	proceeding, and that the transcript is a true and
6	accurate transcription of my shorthand notes to the best
7	of my ability taken while listening to the provided
8	recording.
9	
10	Dated this 28th day of December, 2020.
11	$\Lambda \cap \Lambda$
12	Many by S
13	The state of the s
14	
15	
16	JACKIE MENTECKY
17	
18	
19	
20	
21	
22	
23	
24	
25	

Exhibit 91

Case 1:21-cv-00040 Document 1-90 Filed 01/08/21 Page 2 of 2

screenshot-twitter.com-2021.01.06-14_12_32 https://twitter.com/SidneyPowell1/status/1325820207768633345?s=20 06.01.2021



Exhibit 92

Case 1:21-cv-00040 Document 1-91 Filed 01/08/21 Page 2 of 2

screenshot-twitter.com-2021.01.06-14_13_15 https://twitter.com/SidneyPowell1/status/1326622101772570624?s=20 06.01.2021



Exhibit 93

Case 1:21-cv-00040 Document 1-92 Filed 01/08/21 Page 2 of 9 Sidney Powell with Lou Dobbs Release the Kraken

```
1
 2
 3
 4
 5
                               FILE NAME:
 6
           Sidney Powell With Lou Dobbs Release The Kraken
 7
                                (8:29 min)
 8
 9
10
11
12
                TRANSCRIPT OF VIDEO-RECORDED INTERVIEW
13
                             SIDNEY POWELL
14
                               LOU DOBBS
15
16
17
18
19
20
21
22
23
24
    Transcribed By:
    TERRI NESTORE
25
    CSR No. 5614, RPR, CRR
```

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

2.2

23

24

25

LOU DOBBS: Breaking news now. Dominion Voting Systems say they categorically deny any and all of President Trump's claims that their voting machines caused any voter fraud in key swing states or electoral fraud, but reports contradict that claim. In 2016 a senior executive at Dominion told the Illinois State Board of Elections that it is possible to bypass their election system software. Here's what the vice president of engineering at Dominion at that time, Eric Coomer, told the Board during a meeting in good old Cook County. ERIC COOMER: No, we are not allowed to do routine updates without having to go through a recertification effort, but we do routinely give guidance on how to best secure systems, and also going back again to the final mitigation against all of this is a robust auditing and canvassing process, which all of our jurisdictions have employed. LOU DOBBS: Coomer said no updates can be done without recertification, as you heard. Mr. Coomer's assurances of a secure system, however, are contradicted by the fact that various vendors, election officials and others reportedly can access the voting machine code without an update being required, and we know that there were updates on those machines the day before the

1 election. Well, joining us tonight is Sidney Powell, a 2 3 member of President Trump's legal team, General Flynn's 4 defense attorney, a great American and prominent appellate 5 Great to have you with us, Sidney. 6 SIDNEY POWELL: Thank you, Lou. Let's start with Dominion, a straight LOU DOBBS: out disavowal of any claim of fraud against the company, 8 9 its software or machines. Your reaction. SIDNEY POWELL: Well, I can hardly wait to put 10 11 forth all the evidence we have collected on Dominion, 12 starting with the fact it was created to produce altered 13 voting results in Venezuela for Hugo Chavez and then 14 shipped internationally to manipulate votes for purchase in other countries, including this one. 15 16 It was funded by money from Venezuela and Cuba, 17 and China has a role in it also. So if you want to talk 18 about foreign election interference, we certainly have it 19 now. We have staggering statistical evidence, we have staggering testimony from witnesses, including one who was 20 21 personally in briefings when all of this was discussed and planned, beginning with Hugo Chavez and how it was 2.2 23 designed there and then saw it happening in this country. 24 As soon as the states shut down on election night 25 and stopped counting, those are the states where the most

1 egregious problems occurred. We also need to look at and we're beginning to 2 3 collect evidence on the financial interests of some of the 4 governors and Secretaries of State who actually bought 5 into the Dominion Systems, surprisingly enough -- hunter 6 Biden type graft to line their own pockets by a getting voting machine in that would either make sure their election was successful or they got money for their family 8 9 from it. Well, that's straightforward. 10 LOU DOBBS: 11 take -- you're going to have to be quick to go through and 12 to produce that investigation and the results of it. 13 The December -- the December deadlines are 14 approaching for electors and just as we saw in 2000 with 15 Bush v. Gore. How critical are those deadlines and how 16 urgent does that make your investigation and discovery? 17 SIDNEY POWELL: Well, for fraud this serious, I 18 think even if the states are stupid enough to go ahead and 19 certify the votes where we know the machines were 20 operating and producing altered election results, if 21 they're stupid enough to do that, then they will be set aside by the fraud also. I mean, we are talking about 22 hundreds of thousands of votes. 23 24 President Trump won this election in a landslide. 25 It's going to be irrefutable, and we are -- patriots are

```
1
   coming forward all -- every day, all day, faster than we
    can collect their information, with testimony they're
 3
   willing to give under oath about how their votes were
 4
    stolen and how the machines operated.
 5
             They were updated the night of the election,
    sometimes after the election. We've got statistical
 6
    evidence that shows hundreds of thousands of votes being
    just put in and replicated.
 8
 9
             It's going to be -- there needs to be a massive
10
    criminal investigation and it's going to affect millions
11
   of voters and elections.
12
             LOU DOBBS:
                         With these allegations, these
13
    charges, is the FBI already carrying out an investigation
    of these voting companies and where their servers are
14
    domiciled and in at least two instances -- three
15
16
    instances, we know they're in foreign countries.
17
             Tell us where the Justice Department is in all of
18
    this.
19
             SIDNEY POWELL: I wish I knew.
                                             I'm not on the
20
    inside, so I'm not privy to that information.
                                                    I know that
21
    even democratic senators and Congress people for years
   have reported problems with this system to the FBI and to
2.2
23
    the government and nobody's done a blooming thing about
24
   it.
25
             The people in the election security part of the
```

1 Department of Homeland Security need to be fired 2 yesterday. They're absolutely ridiculous. 3 Of course Chris Wray needs to be fired too 4 because the only FBI interview of any witness was to 5 intimidate him and try to get him to change his truthful testimony, for hours, by an anti-Trump FBI agent. 6 They still have politics infecting the FBI, instead of just following the law. 8 9 We are on the precipice of -- this is essentially a new American revolution, and anybody who wants this 10 11 country to remain free needs to step up right now. These are federal felonies. Altering a vote or 12 13 changing a ballot is a federal felony. People need to 14 come forward now and get on the right side of this issue 15 and report the fraud they know existed in Dominion Voting 16 Systems, because that's what it was created to do. 17 its sole original purpose. It has been used all over the 18 world to defy the will of people who wanted freedom. 19 LOU DOBBS: Sidney, at the outset of this broadcast I said that this is the culmination of what has 20 21 been a over a four-year effort to overthrow this president; to first deny his candidacy, the election, but 2.2 23 then to overthrow his presidency. This looks like the effort to carry out an endgame in the effort against him. 24 25 Do you concur?

1 SIDNEY POWELL: Oh, absolutely. And it's been 2 organized and conducted with the help of Silicon Valley 3 people, the big tech companies, the social media 4 companies, and even the media companies, and I'm going to 5 release the kraken. Well, good, because this is an 6 LOU DOBBS: 7 extraordinary and such a dangerous moment in our history. 8 I really am very concerned for the country, I am 9 very concerned for all Americans, and I have a feeling that most democrats are first Americans, and not 10 11 democrats. They have to be at alarmed as any one of us. 12 Sidney, we're glad that you are on the charge to straighten out all of this. It is a foul mess and it is 13 14 far more sinister than any of us could have imagined, even 15 over the course of the past four years. 16 You get the last word, Sidney. 17 SIDNEY POWELL: It is indeed a very foul mess. 18 It is farther and wider and deeper than we ever 19 thought, but we are going to go after it and I am going to 20 expose every one of them. 21 Sidney Powell, thanks for being with LOU DOBBS: 2.2 us, and thanks for all that you're doing. 23 (End of recording.) 24 25

1	CERTIFICATE
2	
3	
4	I, TERRI NESTORE, Certified Shorthand Reporter/
5	Transcriptionist, do hereby certify that I was authorized
6	to transcribe the foregoing recorded proceeding, and that
7	the transcript is a true and accurate transcription of my
8	shorthand notes, to the best of my ability, taken while
9	listening to the provided recording.
10	
11	I further certify that I am not of counsel or
12	attorney for either or any of the parties to said
13	proceedings, nor in any way interested in the events of
14	this cause, and that I am not related to any of the
15	parties thereto.
16	
17	
18	Dated this 18th day of December, 2020.
19	
20	TERLI NESTORS
21	TERRI NESTORE, CSR 5614, RPR, CRR
22	
23	
24	
25	

Exhibit 94

Case 1:21-cv-00040 Document 1-93 Filed 01/08/21 Page 2 of 7 One on one with Sidney Powell

```
1
 2
 3
 4
 5
                                FILE NAME:
 6
                     One-on-one With Sidney Powell
 7
                                (5:08 min)
 8
 9
10
11
12
                TRANSCRIPT OF VIDEO-RECORDED INTERVIEW
13
                             SIDNEY POWELL
14
                               ERIC BOLLING
15
16
17
18
19
20
21
22
23
24
    Transcribed By:
    TERRI NESTORE
25
    CSR No. 5614, RPR, CRR
```

1 ERIC BOLLING: Former federal prosecutor and 2 General Michael Flynn's attorney, Sidney Powell. 3 Thank you for joining us. 4 Counsel, tell us a little bit about the 5 challenges that the Trump administration is facing, and 6 what are your thoughts on whether or not they will be able 7 to flip any states. 8 SIDNEY POWELL: They're facing an election that 9 was absolutely rigged. It is -- we are soaking in 10 information through fire hoses of complicated mathematical 11 alterations to the votes. We have identified the system 12 capability that does it. It does in fact exist, 13 regardless of what the name of it is. It works through the Dominion company's voting machines that were in 30 14 15 states and does indeed alter and flip voting results. 16 ERIC BOLLING: So can you tell me right there --17 I understand that. 18 So there are these Dominion machines that were 19 voting machines and as you point out, they're in multi, 20 multiple counties across the country that may have 21 So how do you know this? Where is the --2.2 listen, I'm not pushing back on you because I know 23 everyone's going crazy right now, but is there proof of 24 that? 25 Well, the Dominion machines SIDNEY POWELL: Yes.

6

8

9

10

12

15

16

18

19

20

1 are in 30 states. We're identifying the companies that created the software. They have done this in other 3 countries around the world. It's incredibly disturbing, and we will hopefully have evidence of it before the end 4 of the week that we can produce publicly. And the Justice Department and the FBI and the 7 intelligence agencies, I think have known about this before, so why nothing's been done about it yet is beyond my comprehension, but it's fixing to go public because I'm not going to stand by and watch the American public be 11 defrauded of their chosen leader in a free country, a country that's supposed to be free, not run by Venezuela 13 or China. 14 ERIC BOLLING: Sidney, very important information, news, you're breaking here. Is it a software glitch or something more nefarious? 17 SIDNEY POWELL: No, it's a feature of the system that was designed with a backdoor so that people could watch in realtime and calculate with an algorithm how many votes they needed to change to make the result they wanted 2.1 to create. 2.2 ERIC BOLLING: How did you find out about this? 23 SIDNEY POWELL: People have come to me with 24 information. I think when people realize there's somebody 25 they can trust, that will actually do something about it,

1 they speak up. 2 We have a lot of patriots in this country. 3 are absolutely fed up to the gills with corruption at 4 every level of government. They have no trust in our public institutions now, and we will not let this election 5 6 be stolen or any cheating to survive. ERIC BOLLING: So let me get this straight -it's a real important point here. Dominion voting 8 9 machines were in numerous states, numerous counties. 10 There's some sort of software backdoor, not unlike most 11 phones will have a backdoor, but this will actually 12 calculate and tell the person accessing the backdoor what 13 type of voting percentages and what type of numbers are 14 needed to change the win for a certain party, for a 15 certain candidate? 16 SIDNEY POWELL: Exactly. They can watch the 17 voting realtime, they run a computer algorithm on it as 18 needed to either flip votes, take votes out or alter the 19 votes to make a candidate win. 20 ERIC BOLLING: So that's different. Now you're 21 And I just really want to be -- this is even different. 2.2 very careful here and be very meticulous about this. 23 one thing to be able to watch it and decide how much more input you need to change, to change the number, but now 24 25 you're saying there's an actual way to change the total,

```
1
   the vote tallies within the system?
 2
             SIDNEY POWELL: That's exactly right.
 3
             ERIC BOLLING: That is a very, very big claim
 4
            I mean, that would be voter fraud defined, right
    there.
 5
            What's the next step?
    there.
             SIDNEY POWELL: It's massive criminal voter
 6
 7
    fraud, writ large, across at least 29 states it could have
   been happening. Any time a voting machine was connected
 8
 9
   to the internet -- and we have evidence that many were --
10
    it was obviously happening.
11
             It's obvious from the algorithm and the
12
    statistics that our experts are tracking out for batches
13
    of votes and when the curves changed, and it's going to
14
   blow the mind of everyone in this country when we get it
15
   all together and can explain it, with the affidavits and
16
    the experts that have come forward.
17
             ERIC BOLLING: All right. Sidney, we're going to
    leave it there and we're going to look into it and we're
18
19
    going to watch for further information coming out from
20
   your camp, I quess Rudy Giuliani's camp as well, the Trump
21
           So Sidney Powell, thank you very much.
2.2
             SIDNEY POWELL: Thank you.
23
             ERIC BOLLING: America This Week has reached out
24
    to Dominion Voting for a response --
25
             (End of recording.)
```

1	CERTIFICATE
2	
3	
4	I, TERRI NESTORE, Certified Shorthand Reporter/
5	Transcriptionist, do hereby certify that I was authorized
6	to transcribe the foregoing recorded proceeding, and that
7	the transcript is a true and accurate transcription of my
8	shorthand notes, to the best of my ability, taken while
9	listening to the provided recording.
10	
11	I further certify that I am not of counsel or
12	attorney for either or any of the parties to said
13	proceedings, nor in any way interested in the events of
14	this cause, and that I am not related to any of the
15	parties thereto.
16	
17	
18	Dated this 18th day of December, 2020.
19	
20	TERLI NESTORS
21	TERRI NESTORE, CSR 5614, RPR, CRR
22	
23	
24	
25	

Exhibit 95

```
1
 2
 3
 4
 5
                               FILE NAME:
 6
    Fox News Attorney Powell on election legal challenges that
 7
                  remain active in several states
 8
                              (11:50 min)
 9
10
11
12
                TRANSCRIPT OF VIDEO-RECORDED INTERVIEW
13
                             SIDNEY POWELL
14
                            MARIA BARTIROMO
15
16
17
18
19
20
21
22
23
24
    Transcribed By:
    TERRI NESTORE
25
    CSR No. 5614, RPR, CRR
```

3

5

6

8

9

11

16

17

18

19

1 MARIA BARTIROMO: According to public records, Dominion voting machines are used in 2000 jurisdictions in 30 states. According to experts, if one site has a flaw, other sites are likely to as well, which is why Texas 4 rejected using Dominion software three times, raising concerns that the system was not safe from fraudulent or unauthorized manipulation. That's troubling, given we already know that at least two software glitches in Georgia and Michigan occurred on election night. 10 Attorney Sidney Powell is leading the charge against Dominion and she says she has enough evidence of 12 fraud to launch a massive criminal investigation. 13 Sidney, thanks very much for being here. 14 We appreciate your time this morning. 15 I want to get right into it. We just heard about the software made by Smartmatic from Rudy, and I want to get your take on what you and I spoke about just a few minutes ago, and that is a gentleman named Peter Neffenger. Tell me how he fits into all of this. Well, he's listed as --20 SIDNEY POWELL: Yes. 21 it's former Admiral Peter Neffenger or Retired Admiral Peter Neffenger. He is president and on the board of 22 23 directors of Smartmatic, and it just so happens he's on 24 Mr. Biden's presidential transition team that's going to 25 be nonexistent because we're fixing to overturn the

3

4

5

6

8

9

10

11

12

13

14

15

16

17

18

19

20

21

2.2

23

24

25

results of the election in multiple states, and President Trump won by not just hundreds of thousands of votes, but by millions of votes that were shifted by this software that was designed expressly for that purpose. We have sworn witness testimony of why the software was designed. It was designed to rig elections. He was fully briefed on it, he saw it happen in other It was exported internationally for profit by countries. the people that are behind Smartmatic and Dominion. They did this on purpose. It was calculated. They've done it before. We have evidence from 2016 in California. We have so much evidence, I feel like it's coming in through a fire hose. So Sidney, you feel that MARIA BARTIROMO: Wow. you will be able to prove this. Do you have the software in your possession, do you have the hardware in your possession? How will you prove this, Sidney? SIDNEY POWELL: Well, I've got lots of ways to prove it, Maria, but I'm not going to tell, on national TV, what all we have. I just can't do that. MARIA BARTIROMO: Okay, but you have a very small time frame here. The elections are supposed to be certified in early December. Do you believe that you can present this to the courts and be successful, within this just couple of weeks?

Powell, who's part of President Trump's legal team.

Welcome back. We are back with attorney Sidney

short break and come back on that.

23

24

25

Sidney, before we went to the break, we talked about -- you said that there may have been kickbacks to some people who accepted the Dominion software.

Tell me what you mean.

2.2

evidence now from various whistleblowers that are aware of substantial sums of money being given to family members of State officials who bought this software. I mean we're talking about hundred million dollar packages for new voting machines suddenly in multiple states, and benefits ranging from financial benefits for family members to sort of what I would call election insurance because they know that they can win the election if they are using that software.

It's really an insidious, corrupt system and I can't tell you how livid I am with our government for not paying attention to complaints even brought by democrats; Carolyn Maloney, Elizabeth Warren, Amy Klobuchar over the last several years, in written letters, with expert reports and some documentation of how corrupt this software is, and nobody in our government has paid any attention to it? Which makes me wonder how much the CIA has used it for its own benefit in different places, and why Gina Haspel is still there in the CIA is beyond my comprehension. She should be fired immediately.

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

2.2

23

24

25

MARIA BARTIROMO: Which governor or which government official accepted hundreds of millions of dollars in benefits for their family as they took on this software? SIDNEY POWELL: If I said hundreds of millions of dollars there, I misspoke. I don't know the exact amount of money yet. We are still collecting the evidence on that, but it's more than one. MARIA BARTIROMO: Okay. So you can't say who you believe took kickbacks. What is the CIA's role? Why do you think Gina Haspel should be fired immediately? You're saying that the CIA is behind the Dominion or Smartmatic voting software as well? SIDNEY POWELL: Well, the CIA and the FBI and other government organizations have received multiple reports of wrongdoing and failures and vulnerabilities in this company's product. Their own manual, if you sat down and read it, would explain how and why no honest person would use this system. And it's not just Dominion. There are other companies in the voting machine business in this country too that may very well, and are likely using the same software. We've detected voting irregularities that are inexplicable and align with these problems in other states that think they have valid systems, but the people who bought the Dominion system for

2.2

sure knew exactly what they were getting. It should never have been installed anywhere, and we are going to show the public exactly how rotten the entire state is.

MARIA BARTIROMO: Now, I have spoken with a few whistleblowers myself this weekend and one source, who is an IT specialist, told me that he knows the software and specifically advised people in Texas, officials in Texas, not to use it, and yet he was overruled.

He said that there was an unusual patch that was put into the software while it was live, and it's highly unusual to put a patch in there.

Is that what you're referring to? Tell me how

Is that what you're referring to? Tell me how it's done and how these backdoors work.

SIDNEY POWELL: Okay, that's part of it.

They can stick a thumb drive in the machine or upload software to it, even from the internet. They can do it from Germany or Venezuela even. They can remote access anything. They can watch votes in realtime. They can shift votes in realtime.

We've identified mathematically the exact algorithm they used and planned to use from the beginning to modify the votes in this case to make sure Biden won. That's why he said he didn't need your votes now. He would need you later. He was right. I mean, in his demented state, he had no filter and he was speaking the

1 truth more than once, including when he said he had the 2 largest voter fraud organization ever. Well, it's massive 3 election fraud. It's going to undue the entire election. 4 And they can do anything they want with the They can have the machines not read the signature, 5 6 they can have the machines not read the down ballot, they can make the machines read and catalog only the Biden It's like drag and drop whatever you want, 8 9 wherever you want, upload votes. 10 MARIA BARTIROMO: Yeah. 11 SIDNEY POWELL: In fact, we've got math in 12 Michigan and Pennsylvania, I think it is, that all of a 13 sudden hundreds of thousands of votes, at a 67 percent 14 ratio for Biden, 23 percent for Trump --15 MARIA BARTIROMO: Yep. 16 SIDNEY POWELL: -- were uploaded multiple times 17 into the system. 18 And Sidney, you say you have an MARIA BARTIROMO: 19 affidavit from someone who knows how the system works and 20 was there with the planning of it. 21 You believe you can prove this in court? 22 SIDNEY POWELL: Oh, yes. We have a sworn --23 essentially a sworn statement from a witness who knew 24 exactly how it worked from the beginning, why it was 25 designed to work that way and saw, when things started

```
1
    shutting down and they stopped counting the votes here,
 2
    that was the same play that had worked in other countries.
 3
             MARIA BARTIROMO: Wow. This is explosive and we
 4
    certainly will continue to follow it.
 5
             Sidney, thank you so much for your work. We will
 6
    be catching up with you soon. Thank you so much.
 7
             (End of recording.)
 8
 9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
```

1	CERTIFICATE
2	
3	
4	I, TERRI NESTORE, Certified Shorthand Reporter/
5	Transcriptionist, do hereby certify that I was authorized
6	to transcribe the foregoing recorded proceeding, and that
7	the transcript is a true and accurate transcription of my
8	shorthand notes, to the best of my ability, taken while
9	listening to the provided recording.
10	
11	I further certify that I am not of counsel or
12	attorney for either or any of the parties to said
13	proceedings, nor in any way interested in the events of
14	this cause, and that I am not related to any of the
15	parties thereto.
16	
17	
18	Dated this 17th day of December, 2020.
19	
20	TERLI NESTORS
21	TERRI NESTORE, CSR 5614, RPR, CRR
22	IBRRE NEBTORE, CBR 3011, REIR, CRR
23	
24	
25	

Exhibit 96

Case 1:21-cv-00040 Document 1-95 Filed 01/08/21 Page 2 of 16 Rush Limbaugh Show Podcast November 16, 2020

1	
2	
3	
4	
5	FILE NAME:
6	THE RUSH LIMBAUGH SHOW PODCAST - November 16, 2020
7	
8	
9	
10	
11	
12	TRANSCRIPT OF VIDEO-RECORDED INTERVIEW
13	SIDNEY POWELL
14	MARK STEYN
15	
16	
17	
18	
19	
20	
21	
22	
23	
24	Transcribed By: TERRI NESTORE
25	CSR No. 5614, RPR, CRR

1 Mark Steyn in for Rush on America's MARK STEYN: 2 number one radio show. 3 You may have read stories in the media over the 4 weekend about the pressure that Trump lawyers are 5 calling -- coming under to bail from the case and abandon 6 their client. One lawyer we can say certainly who is not going to do that is Sidney Powell. She was last on with me as a tireless champion of her client Michael Flynn. 8 9 She's now a tireless champion of her new client, 10 Donald J. Trump in some of these postelection legal 11 battles and Sidney, you've become very concerned about 12 this Canadian company, Dominion Voting Systems. 13 As I said on the show, this show last week, it's 14 illegal for a Canadian to give a C-note to a presidential 15 candidate but apparently it's not in the least bit illegal 16 for a Canadian company to end up running American 17 elections in 33 states. What's the problem for you with 18 this Dominion Voting Systems. 19 SIDNEY POWELL: Well, there are so many problems, Mark, it would be hard to articulate all of them. 20 21 Their system was specifically created and 2.2 designed by Venezuelan money and interest to rig elections 23 for Hugo Chavez and then for Maduro. It was exported 24 internationally, I understand, to rig an election in 25 Argentina, and it has been used to rig this election for

1 -- to make it appear the votes were for Mr. Biden, when 2 Donald Trump won overwhelmingly, and I'm in the process of 3 collecting evidence through a firehose, to the point it 4 feels like a tsunami now, of honest, patriotic people; 5 American citizens who are coming forward to tell us 6 exactly what was going on. 7 And I just got word today that a hundred Dominion employees have even taken any affiliation with Dominion 8 9 off their LinkedIn accounts, and Dominion is scrubbing 10 names of people like crazy. 11 MARK STEYN: Right, right. And it started -- it 12 only came out because I think a county clerk happened to 13 notice that 6,000 Trump votes had been transferred to Joe 14 Biden, I believe in Michigan, but presumably lesser --15 SIDNEY POWELL: It also came out because some of 16 my math experts who I know very well, immediately 17 identified the algorithm that was being run to change the 18 vote. 19 MARK STEYN: Right. 20 SIDNEY POWELL: So that any number of batches of 21 votes were changed by the machine which, by its own 22 manual, tells people it can do that. It was changed to 23 run 67 percent for Biden and votes were injected in that 24 number by the hundreds of thousands multiple times. The 25 exact same number and ratio were injected like three times

in Wisconsin and twice in Michigan or vice versa a couple 1 2 of -- 20 minutes apart or something. 3 MARK STEYN: Yeah. 4 SIDNEY POWELL: It's absurd. And for people to say there's no evidence of fraud are the people that want 5 6 to cover up the fraud for whatever their personal interests are. We also have some evidence coming in that people who bought these Dominion system for their states, 8 9 got special benefits on the side. 10 MARK STEYN: Right. 11 SIDNEY POWELL: And -- yeah, I mean the level and 12 width of the corruption is what the American people have 13 felt for a long time but we're just now getting people to 14 come forward because it's so bad and they've realized that 15 I'm here and I will fight for it until we get it out 16 there. 17 MARK STEYN: I was very interested by this 18 business of the algorithm because I hadn't realized until 19 then -- I'd heard of this company, but the -- in Canada, 20 they're just tabulators; in other words, they just run 21 optical scanners that scan paper ballots. So if you have an argument about the results, as I think they did in 22 23 Nova Scotia-New Brunswick a couple of years back, they've actually got the hardcore paper ballots and they go back 24 25 and count them manually but in America, it's completely

1 different machines they're running, which are actually 2 voting machines and not just these optical scanners. 3 You've been going on about Gina Haspel at the 4 I mean, the deep state security guys who certified CIA. 5 that this is the cleanest election ever run in America, 6 are they the guys --7 SIDNEY POWELL: They need to be fired. 8 MARK STEYN: Yeah. 9 SIDNEY POWELL: They need to be fired. I don't 10 know whose payroll they're on but they need to be fired 11 yesterday. Democrats, Elizabeth Warren and Amy Klobuchar, 12 were complaining about this several years ago. 13 Maloney wrote a letter to people about it years ago. 14 They're even scrubbing the articles they cited 15 from the internet. We've gone to check on several links 16 This is very widespread, and I have no and they're gone. 17 doubt at this point it involves the tech companies at 18 Silicon Valley, who are also trying to suppress our free 19 speech on all of these issues to cover their own 20 you-know-what's, and I am livid about all of it, I am 21 livid about the level of corruption, I am livid that the 2.2 FBI and the CIA haven't done anything about the complaints 23 they've received, which just makes me want to know even 24 more who's been paid what and who is responsible for all 25 of this and who's paid whom to get their -- buy their

1 elections. 2 And as you say, the media and the MARK STEYN: 3 CIA and everybody else say, ah, give it up, there's 4 nothing to see here. What do you think -- I take it you 5 agree that this case ultimately is going to wind up before 6 those nine guys on the Supreme Court. Do you think they're going to be as eager to just sweep it under the rug? 8 9 SIDNEY POWELL: I don't think so, Mark. I think 10 the evidence is going to be so overwhelming, and I would 11 warn any state right now that thinks they're going to certify this election, to rethink it very seriously 12 13 because what they're certifying is their own fraud and 14 their own complicity in fraud and I wouldn't -- I might even mount a class action suit later to sue them 15 16 themselves for their participation in it. 17 It's ridiculous. 18 The legislators in the states need to take 19 control right now and reject the certifications of 20 especially the swing states that were so heavily 21 influenced by these hundreds of thousands of vote changes. 2.2 And the people in Smartec's (sic) own manual 23 tells you they can do this, they can change any vote they 24 want to change, they can reallocate ID from one vote to 25 another, they can take batches of votes and trash them.

```
1
   If they were for Trump, they can add votes for Biden.
   They can be manipulated any way they want to be
 3
   manipulated, and they had VPN connections and access and I
 4
   think Raheem Kassam actually tweeted a message yesterday
 5
   or a picture yesterday of Glenn Simpson looking behind a
    string of Dominion voting machines.
 6
             MARK STEYN: Yeah. You said, if I understood you
    correctly, that they can actually program the percentages
 8
 9
   of as it were, they can actually override whatever votes
   are in the machine and --
10
11
             SIDNEY POWELL: Exactly.
             MARK STEYN: -- adjust them up and down until
12
13
    they reach the -- why would that be a feature of a voting
14
   machine?
15
             SIDNEY POWELL: Because it was created to do that
16
    to begin with. That's how Hugo Chavez and Maduro have
17
   ensured they won every Venezuelan election.
18
             MARK STEYN:
                          So somehow a Canadian company wound
19
   up putting Venezuelan counting machines in 33 American
20
    States.
             That's the upshot of that, Sidney.
21
             SIDNEY POWELL: Yeah.
                                    It was all created in
2.2
   Venezuela and designed to do this very thing, and they've
23
    installed Venezuelan machines and then the votes actually
24
   go to Barcelona, Spain, and Frankfurt, Germany, where they
25
    can be further manipulated before they're sent back to be
```

1 reported on AP and the New York Times and all that. 2 It was caught this big this time was because 3 Donald Trump's lead was so overwhelming, they didn't 4 calculate the algorithm high enough, and that's why they 5 had to stop them. MARK STEYN: Just a minute there, Sidney. 6 I had 7 no idea about that. These votes are actually counted in 8 -- they travel halfway around the world to Barcelona 9 before they're counted. I want to come back with you. 10 Hang on, please, Sidney. I want to come back and talk 11 about that some more because that's extremely important. 12 Mark Steyn for Rush. 13 More with Sidney Powell straight ahead. 14 We have with us the fearless attorney for both 15 Michael Flynn and the president in his legal challenges, 16 Sidney Powell. 17 And as Sidney mentioned, they're talking about 18 some class action suits to prevent the states prematurely 19 certifying the election, and if you have some evidence of 20 electoral fraud, you can go to Sidney's Website, 21 defendingtherepublic.org. It's well named, 2.2 defendingtherepublic.org, because Sidney will be defending 23 it when most everybody else has fled. If you have 24 evidence of electoral fraud, particularly in these 25 critical swing states, then do go to that website.

1	Sidney, you said something incredible to me
2	because as odd as it is that these foreign made machines,
3	Canadian machines with Venezuelan algorithms are now in
4	33
5	SIDNEY POWELL: You might as well call them
6	Venezuelan machines, because that's essentially what they
7	are. There are a number of different companies to do this
8	and yes, we have Venezuelan communists influenced by Cuban
9	communists counting our votes and deciding how our
10	election is going to come out. It's an absolute outrage.
11	It should be being investigated by the highest of our
12	Intel investigators, preferably military because it's a
13	national security threat, and that's exactly why they've
14	done this. Oh, and don't forget China's influence in all
15	of it too. There's Chinese money and graft in Venezuelan.
16	MARK STEYN: But you mentioned that it actually
17	goes across the Atlantic to Barcelona, and I think you
18	said somewhere else.
19	SIDNEY POWELL: Yeah, Frankfurt.
20	MARK STEYN: Yeah, Frankfurt. So in other words,
21	we've got the Germans and the Spaniards counting American
22	votes too, which would be odd enough if you didn't already
23	have the Canadians, Venezuela. There's everybody but
24	Americans involved.
25	SIDNEY POWELL: Well, the Spanish part is

1 actually -- those parts are actually controlled by the 2 Venezuelans too, the counting centers over there are 3 controlled by the Venezuelan money. 4 MARK STEYN: But you're a lawyer and you know 5 that in any law, even in the most trivial lawsuit, chain 6 of custody of the evidence is the most important thing, you know; that a photocopy of a photocopy of what might have been an original document 37 versions 8 9 earlier is less persuasive as evidence than the real 10 thing, so why do we have like a complete contempt of chain 11 of custody here, where these votes are sent actually into 12 foreign jurisdictions before they eventually return as 13 hard numbers? 14 SIDNEY POWELL: Right. And they can -- there are 15 multiple means of how they alter it. They alter it to 16 begin with by running the algorithm where they want to run 17 it, but they can also alter it by trashing votes, adding 18 votes, and then if they don't like it still then, they can 19 change it again in Barcelona. MARK STEYN: 20 So in other words, whatever 21 shenanigans -- to use the euphemism people seem to prefer -- whatever shenanigans take place in a precinct in 2.2 23 Michigan, if that's insufficient, they can change it yet 24 again while the so-called vote is out of the country? 25 SIDNEY POWELL: Right. The hand count in Georgia

2

3

4

5

6

8

9

10

11

12

13

14

15

16

17

18

19

20

21

2.2

23

24

25

that they're pretending to do now, they're going to try to use that to promote the argument that the Dominion fraud software stuff is a hoax. That's baloney. They did all kinds of different things there that include kind of closing out republican accounts and doing provisional ballots for people that then disappeared, and we've got to have access to the machines themselves to get the software and examine it but we know there were, quote, glitches in Georgia too, and any time there was a glitch like that, there was software probably uploaded that changed things. They can change it over the internet. It should never have had an internet connection. Patches were put in like the day before the election and they were never The machines aren't supposed to be touched for certified. ages before the election. That's a violation of law, by itself. I mean -- but we also have -- at least I've been told that there are special concerns about the governor of Georgia and the Secretary of State having received some kind of personal benefit for rushing through the purchase of the Dominion machines into the state. MARK STEYN: You said something else interesting there, that they actually were connected to the internet because last time round we were told, when there was all

this stuff about the Russian collusion and all the rest of 1 it, that voting machines are safe because voting machines 3 are not online -- they're machines, but they're not -- but 4 some guy sitting in Macedonia or St. Petersburg can't actually hack into it because it's not connected to the 5 6 internet. You're saying that this time round there were 7 machines connected to the internet? 8 SIDNEY POWELL: These machines are so hackable, a 9 15-year-old could do it. MARK STEYN: And does that mean that in the 10 11 lawsuit, you're -- you'd be -- you're asking a judge to 12 actually let some kind of tech experts into the machines 13 themselves to figure out what's been programmed there and 14 what's going on in them? That is definitely one of the 15 SIDNEY POWELL: 16 I can't even tell you at this point things we need. 17 whether it's in any of the existing lawsuits, but I've 18 certainly encouraged people to put them in the ones that 19 they've filed. 20 MARK STEYN: And do you think -- you said you'd 21 thought it was definitely going to the Supreme Court. 22 Everyone seems to think that John Roberts, the 23 chief justice, has no appetite for this and his whole 24 thing is always to, as it were, diminish the significance, 25 to prevent the Supreme Court doing anything like

overturning and being perceived to have overturned an 1 2 election or whatever. 3 Do you think -- I mean, these seem to me to raise 4 absolutely extraordinary issues where essentially foreign 5 actors, we've been told for four years about foreign interference in American elections, and it turns out the 6 entire U.S. election is one great act of multi-foreigner interference. Is that big enough for him to, in a sense, 8 9 not be able to turn down the case? 10 SIDNEY POWELL: If that isn't big enough for him 11 to take the case, he should be impeached. 12 MARK STEYN: There would be a lot of people who 13 would support you on that. Thank you. 14 You always -- you have that thing that really 15 good lawyers have, which is a slight degree of 16 inscrutability, Sidney, when you're being interviewed. 17 Let me just ask you as a final question, do you 18 feel optimistic that the truth is going to get out about 19 this thing? 20 SIDNEY POWELL: I feel very optimistic the truth 21 is going to be -- it will get out. Of course everybody on 2.2 the face of the earth now is trying to suppress it, 23 including people in our own government, but I won't quit 24 until it's out and, you know, release the kraken. Well, indeed, release the kraken. 25 MARK STEYN:

```
1
    Well, God bless you, Sidney, and people can go to
 2
    defendingtherepublic.org, if they want to know more about
 3
    this.
 4
             SIDNEY POWELL: Yes.
                                    Thank you so much, Mark.
 5
             MARK STEYN:
                           Thanks a lot, Sidney.
 6
             It's always a pleasure, even in trying times.
 7
             Defendingtherepublic.org. Sidney really ought to
8
    take releasethekraken.org as well.
 9
             (End of interview.)
10
11
12
13
14
15
16
17
18
19
20
21
2.2
23
24
25
```

1	CERTIFICATE
2	
3	
4	I, TERRI NESTORE, Certified Shorthand Reporter/
5	Transcriptionist, do hereby certify that I was authorized
6	to transcribe the foregoing recorded proceeding, and that
7	the transcript is a true and accurate transcription of my
8	shorthand notes, to the best of my ability, taken while
9	listening to the provided recording.
10	
11	I further certify that I am not of counsel or
12	attorney for either or any of the parties to said
13	proceedings, nor in any way interested in the events of
14	this cause, and that I am not related to any of the
15	parties thereto.
16	
17	
18	Dated this 18th day of December, 2020.
19	
20	TERLI NESTORS
21	TERRI NESTORE, CSR 5614, RPR, CRR
22	TERRET NEBTORE, CERT SOLI, REIR, CRIC
23	
24	
25	
	1

Exhibit 97

1	
2	
3	
4	
5	FILE NAME:
6	Sidney Powell to Newsmax TV -
7	Dominion Contracts Warrant Criminal Probe
8	(8:19 min)
9	
10	
11	
12	TRANSCRIPT OF VIDEO-RECORDED INTERVIEW
13	SIDNEY POWELL
14	TOM BASILE
15	MARK HALPERIN
16	
17	
18	
19	
20	
21	
22	
23	
24	Transcribed By: TERRI NESTORE
25	CSR No. 5614, RPR, CRR

1 TOM BASILE: Thank you so much, Sidney, for being 2 with us tonight. 3 SIDNEY POWELL: Oh, my pleasure. 4 Thank you for having me. 5 TOM BASILE: The first thing that I really would like to do is get your reaction to this week's news that 6 7 the president has pardoned General Flynn, your client. SIDNEY POWELL: Well, it's a bittersweet 8 9 I felt very strongly, from the day I came into reaction. 10 the case -- actually before that -- that he should be 11 exonerated by our judicial system, and it didn't happen 12 that way, frankly because of the extraordinary political 13 corruption we saw coming out of Judge Sullivan's court and 14 then being affirmed by the D.C. circuit in an absolutely 15 unprecedented proceeding where the judge himself was 16 allowed to seek rehearing en banc before the full court. 17 None of the rules applied. 18 As is the case from the very beginning of the 19 investigation against General Flynn. The FBI broke all 20 the rules to do it, the special counsel broke all the 21 rules to prosecute him, and then the court broke all the 2.2 rules itself to continue the persecution. 23 MARK HALPERIN: Sidney Powell, it's been only a 24 week since you last visited here with Newsmax last 25 Saturday night, and much transpired in between.

2

3

4

5

6

8

9

10

11

12

13

14

15

16

17

18

19

20

21

2.2

23

24

25

Some people say that the president's team distanced themselves from you because in part of the accusations you made that you said you had evidence suggesting that the governor of Georgia, the republican governor, was involved in a conspiracy. I'm wondering if, upon reflection, that's something you stand by and something you'll continue to pursue. SIDNEY POWELL: Well, what I said and I thought I said and intended to say is there should be an investigation, a thorough criminal investigation, frankly, of everyone involved in acquiring the Dominion system for the State of Georgia, and frankly for every other state, given how appalling the system is and the fact that it was designed to manipulate the votes and destroy the real votes of American citizens who were casting legal votes. That applies to Georgia as well. I have serious concerns that certain people -- in fact, one lawyer told me that one of his clients knew of money or benefits being paid to family members of those who signed the contract for Georgia, and I believe it was a no bid contract that Georgia awarded for the Dominion Systems, a hundred million dollar no bid contract. We know from Pennsylvania, for example, that the governor of Pennsylvania mandated that they accept the contract with Dominion, so there's an investigation that

should be had there because the legislature opposed it.

2.2

And I think there are multiple people in the Secretary of State's office in Georgia and others who should be investigated in Georgia for what benefits they might have received from giving Dominion the \$100 million no bid contract.

TOM BASILE: Sidney, this week you filed cases in Georgia and in Michigan, alleging widespread fraud and illegality in those races. You make a number of specific allegations and you also provide specific evidence which would probably come as a surprise to a lot of folks in the left wing press.

Can you discuss your Georgia case, since the margin between Trump and Biden there is closer, and I think that you lay out a number of different avenues for success there that could be, again, outcome determinative and, you know, in particularly talk about how Georgia violated its own law that caused the processing of defective absentee ballots.

SIDNEY POWELL: Yes, Georgia set a completely different standard for its mail-in ballots than it had for its real absentee ballots and frankly, all across the country there should never have been any sort of separate, quote, mail-in ballot system.

The absentee ballot process that had been

2.2

entire state.

approved by legislatures in virtually every state was appropriate and could have been used for any reason people could not get to the polls without this wholesale mail-out and then mail back in your ballot, which was simply an invitation for massive fraud, and that's exactly what we've experienced.

We're seeing every manner and means of fraudulent voting you can possibly think of and many you couldn't, from the system applied in Georgia; everything from the point shaving system that Dominion Systems allows, they weighted votes for president -- or for President Trump at .77 percent and they awarded votes to Biden at something

We've filed an emergency motion now with the federal court to impound all the voting machines and to also require an absolute hand recount that matches signatures, including on all the ballots and envelopes themselves. We believe Georgia has destroyed a number of ballots.

like 1.22 percent. So Biden's votes were weighted an

automatically flipped approximately 2.7 percent of the

additional 20 percent to that of President Trump's, which

vote to Biden in any number of counties, if not across the

There was a massive shredding operation in Cobb County, of which we have video, and if they can't produce

1 the envelopes to go with the ballots, then they've violated federal law, as well as Georgia requirements, and 3 there are all kinds of criminal offenses that arise out of 4 all of this. 5 We've got evidence of significant ballot harvesting, including people being paid to harvest 6 7 ballots. You name it, we've got it. 8 Also of fraudulent ballots being created and 9 brought in. MARK HALPERIN: Sidney Powell, you know full well 10 11 that what a lot of people say about the work you've done 12 so far is that you're making a lot of allegations that are 13 sweeping, some believe that they're not credible, and 14 they're asking for evidence. 15 So just give us one specific piece of evidence 16 that you think illustrates fraud. The clearest piece of 17 evidence you have that illustrates enough fraud to change 18 the results in any one of the states that you believe 19 should be contested. SIDNEY POWELL: Well, there are all kinds of --20 21 MARK HALPERIN: Just one, just give your clearest piece of evidence. What's something that any American 22 23 would see and understand? 24 SIDNEY POWELL: Well, how about the testimony of 25 the person from Venezuela who saw the entire system

1 created to ensure that Maduro and Hugo Chavez never lost 2 another election? He knows exactly how it works. 3 We have other witnesses who know exactly how it 4 works, and that it was designed to enable the sort of vote 5 flipping and switching and the ability to trash votes in large numbers so that Mr. Biden would win without 6 campaigning. He himself said that he had the largest voter fraud operation in the country, and he was right 8 9 about that. We've got video evidence of a number of things. 10 11 We know the Atlanta people lied when they claimed 12 that the pipe -- a pipe burst and kept them from counting 13 votes, and they used that to send people away from the 14 arena or whatever the facility was they were counting in. 15 They completely lied to the public about the timing and 16 the reason for that. There was no pipe burst at all, and 17 we have evidence of three women staying behind after 18 1:00 a.m. to alter the ballots and the vote between 1:00 19 and 4:00 a.m. that morning, I believe. Okay. Well, Sidney Powell --20 TOM BASILE: 21 SIDNEY POWELL: There are multiple pieces of 22 evidence. There are people that witnessed ballot 23 harvesting. We have multiple checks written by people. 24 There are federal criminal offenses that are 25 rampant throughout this, and I am beyond appalled that the

```
1
    Department of Justice and the FBI have not gotten all over
 2
    this.
 3
             TOM BASILE: Well, I, for one, think it would be
 4
    great if we could see some of that video of the shredding
 5
    going on and some of the other things that you're talking
 6
    about. I think the American people would be very, very
 7
    interested in it. Sidney Powell, always a pleasure to
 8
    have you here on Newsmax TV. Thank you very much.
 9
             SIDNEY POWELL:
                             Thank you.
10
             And people who want to help can go to
11
    defendingtherepublic.org and they can see a lot of the
12
    video @tracybeanz on Twitter.
13
             TOM BASILE:
                          All right.
14
             (End of recording.)
15
16
17
18
19
20
21
2.2
23
24
25
```

1	CERTIFICATE
2	
3	
4	I, TERRI NESTORE, Certified Shorthand Reporter/
5	Transcriptionist, do hereby certify that I was authorized
6	to transcribe the foregoing recorded proceeding, and that
7	the transcript is a true and accurate transcription of my
8	shorthand notes, to the best of my ability, taken while
9	listening to the provided recording.
10	
11	I further certify that I am not of counsel or
12	attorney for either or any of the parties to said
13	proceedings, nor in any way interested in the events of
14	this cause, and that I am not related to any of the
15	parties thereto.
16	
17	
18	Dated this 18th day of December, 2020.
19	
20	TERLI NESTORS
21	TERRI NESTORE, CSR 5614, RPR, CRR
22	IBRRE NEBTORE, CBR 3011, REIR, CRR
23	
24	
25	

Exhibit 98

Case 1:21-cv-00040 Document 1-97 Filed 01/08/21 Page 2 of 31 Fredericks Show with Sidney Powell

```
1
 2
 3
 4
                      File:
     Fredericks Show with Sidney Powell
 5
 6
 7
 8
 9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
```

2

3

4

5

6

8

9

10

11

12

13

14

15

16

17

18

19

20

21

2.2

23

24

25

JOHN FREDERICKS: Joining us now is Sidney She has done yeoman's work, as I said, she texted me 3:00 a.m. today when she was going to bed, and I was getting up, and now she's up with me now, filed a massive lawsuit in Arizona yesterday. Hey, Sidney, thanks for being with us. SIDNEY POWELL: Hey, John. Thank you for your support. And Anita is exactly right, there's -- one of the things we were trying to accomplish is to get people to realize that Loeffler and Perdue, among other Georgia leadership, should be out there screaming right now for a special section of the -- session of the legislature, and to get the entire voting system fixed now. And it can't be fixed with Dominion machines. There's nothing reliable about them whatsoever. We're going to have to go to real paper ballots and we're going to have to have, you know, a real hand count of those ballots. JOHN FREDERICKS: So, Sidney, what they're saying is, well, we can't do that in a special session, because you can't change the rules in the middle of the game. But the game is --

```
1
           SIDNEY POWELL:
                           Well, they changed --
 2
           JOHN FREDERICKS: -- rigged --
 3
           SIDNEY POWELL: -- them all in the middle
 4
     of the game last time to make sure they rigged it.
 5
           JOHN FREDERICKS:
                             Exactly.
                                       Exactly.
 6
           SIDNEY POWELL: And the legislature can
 7
     make the rules.
 8
           JOHN FREDERICKS: So you want a special
 9
     session to do this. So, basically, at the rally
10
     yesterday -- and -- and by the way, I've been on
11
     the air ten years, Sidney, I followed everything,
     I go on the ground, I'm in the middle of a 12-city
12
13
     tour in 12 days in Georgia. I was in Alpharetta,
14
     obviously, yesterday, I'm downtown today in
15
     Atlanta for the hearing; we'll be going from
16
     there.
17
           Have you ever seen a movement like this
18
     before ever? 1500 people out there in Alpharetta
19
     cheering on your every word. I mean, they've
20
     had -- they -- they're pissed, and the people are
21
     just -- and the phone calls I'm getting day after
22
     day, people have -- people have had it --
23
           SIDNEY POWELL: Yes.
24
           JOHN FREDERICKS: -- Sidney.
25
           SIDNEY POWELL: Yes, they have had it,
```

```
1
     John.
            And no -- I mean, I was overwhelmed,
 2
     frankly. I had no expectation for the event
 3
     whatsoever.
 4
           And -- I mean, I'm just trying to do what I
 5
     can do to -- to be honest, with respect to all the
     issues. And the pushback that we have been
 6
     getting is -- is really flabbergasting, except
 8
     when you realize that there is so much global
 9
     money behind all of this and -- and, frankly,
10
     malevolence to do the kind of evil that we are
11
     uncovering more of every day.
12
           This is isn't the first year this has been
13
            These machines and algorithms have been
14
     used to rig races all over the world for -- I
15
     don't know how many years, at least 15. We know
16
     that Clinton used it. We know that Obama used it,
     I think in Florida, and maybe other places.
17
18
           I mean, we're getting evidence of every
19
     manner and means of voter and election fraud you
20
     can imagine. But to know now that the voting
21
     machines have been rigged, and it's not just
22
     Dominion, the same DNA code is in most of the
23
     machines that run across the country; maybe not to
     the extent that Dominion did.
24
25
           In fact, I saw a report yesterday that
```

1 Dominion machines averaged six percent more for 2 Biden than any of the others; but that doesn't 3 mean an algorithm wasn't run in the others, also, 4 because they all have that capability and we're 5 seeing signs of fraud in almost every state across 6 the country. JOHN FREDERICKS: So, Sidney Powell, did I just hear you say that the Dominion voting 8 9 machines across the country averaged six percent 10 higher vote count for Biden than the other 11 machines? 12 SIDNEY POWELL: Yes. 13 JOHN FREDERICKS: If -- of course, if -- if 14 the -- if one machine is in Massachusetts and the 15 other that you're comparing it to is in Alabama, 16 obviously, there's going to be a difference. 17 they comparable areas? 18 SIDNEY POWELL: Well, the point is that in 19 -- in places where the other machines were used 20 and sometimes -- the only state I think that was 21 all Dominion or that mandated all Dominion was the 2.2 state of Georgia. 23 Some other states, for example, Arizona 24 only used Dominion in Maricopa County. But the 25 interesting thing is the disparity between the

2

3

4

5

6

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

```
places where Dominion is, and all other places.
And -- and the -- the -- one of the things we know
is, from prior use and testimony, that Dominion
machines auto- -- can flip 2.7 to three percent of
the vote from Trump to Biden easily.
      JOHN FREDERICKS: Uh-huh.
      SIDNEY POWELL: I mean, that's kind of what
they've run many times before. And -- and that
stands to reason that -- that -- that accounts for
the six percent up for Biden, where Dominion
machines were operating.
      JOHN FREDERICKS: Sidney Powell, let me ask
you this, and let's start -- I'm going to start
with Georgia, and then go to Arizona: So in
Georgia right now you -- you filed a 104-page
lawsuit, very detailed. I didn't have a chance to
read it. It's -- it's very, very comprehensive.
      Walk us through when you're going to get a
hearing, what your expectations are, and the time
frame.
      SIDNEY POWELL:
                     Well, the -- the State came
in and argued that we had to sue every district,
every county board person, in the State of Georgia
to seek the relief that we wanted.
                                    We don't think
that's the law.
                 It's not the law.
                                    The Georgia
```

1 Secretary of State bought all the machines for 107 2 million of taxpayer money in a rushed deal. 3 the governor, of course, also. 4 So we had to do an emergency appeal to the 5 11th Circuit, and that -- they granted the expedited review. We've got a brief due tonight 6 7 in that. And meanwhile, we've also filed in Michigan and Wisconsin and Arizona; and we plan to 8 9 file in Pennsylvania. We've got multiple other 10 states to cover. One of the things that's 11 important for people to realize is that many 12 downballot races were affected by the fraud. They 13 could go in and target specific candidates. 14 I'm very upset that John James didn't join 15 our suit in Michigan. He should never have 16 conceded. And the same is true for doing Doug I can't -- I mean, I just -- I don't 17 18 understand it, because I'm 99 percent sure he won 19 his race against Kelly Loeffler. congressional seats were affected. 20 Leon Benjamin 21 in Virginia, I think, was a victim of it. 22 We should have won probably six more Senate 23 seats, and probably ten more House seats. 24 we're going to keep looking and -- and digging out 25 what we can until we get to everything that should

1 have been won. And probably some governor races, 2 too. I mean, it wasn't just -- it wasn't just the 3 presidential race. Of course, that's the most 4 important right now because of the Electoral 5 College issue. But the others can continue to fight, and we need to find out -- we need to 6 7 examine every race and figure out who really 8 should have won, and who perpetrated the fraud. 9 The Department of Justice and NSA and the DNI should be all over this. I don't understand 10 11 what's going on, other than I know some of our 12 three-letter agencies are complicit in it, if not 13 behind it. 14 I mean, Venezuela didn't create this 15 software on its own 20 years ago. 16 JOHN FREDERICKS: Sidney, let me ask you a 17 direct question about evidence. I mean, you've 18 been criticized now in a lot of places in 19 Washington that you've not presented any direct 20 evidence of real voter fraud that somebody could 21 get their arms around and see. 22 How do you respond to that, do you have any 23 direct evidence that you have seen that is really 24 just like -- not a dotted line, but a straight line, real evidence of voter fraud and how this 25

```
1
     election was stolen; do you have any of that?
 2
           SIDNEY POWELL: Yes, we do. And I don't
 3
     understand why people keep saying no evidence,
 4
     except that they want to make people believe
 5
     there's no evidence.
           If you get up in the morning and there's
 6
     six inches of snow on the ground, can you tell
 8
     it's snowed?
                  I -- I mean, that's how stupid it
 9
         And plus --
     is.
10
           JOHN FREDERICKS: Can -- can you --
           SIDNEY POWELL: -- we have direct witnesses
11
     who know why it was created, how it was created,
12
13
     watched it being used, was briefed on all its
14
     features; their own online manual tells people
15
     they can drag and drop votes into the trash.
16
     put them in this thing called an adjudication
17
     file, however many they want to. They can program
18
     the computer not to read signatures and,
19
     therefore, reject thousands of ballots; put them
20
     in quote, an adjudication file, and then just
21
     trash it all.
2.2
           It -- it's -- their own admissions prove
23
     it.
         We've got --
24
           JOHN FREDERICKS: And you have --
25
           SIDNEY POWELL: -- Eric Kumar in a -- in a
```

1 call saying he -- he's got it fixed for Biden; you 2 know, Trump is not going to be President. 3 he's the lead engineer for Dominion. We have the -- the witness who -- who 4 watched it all work. He was in the control room 5 for -- when Dominion was rigging the elections in 6 7 Venezuela. 8 Do -- do people really think that what 9 happens everywhere else in the world with or 10 without CIA help and other nefarious interests 11 can't happen here? Have we learned nothing in the 12 last four years about the lies --13 JOHN FREDERICKS: Uh-huh. 14 SIDNEY POWELL: -- and extent they'll go to 15 steal and cheat and -- and control the money and 16 power of the world? JOHN FREDERICKS: So, Sidney, you have --17 18 do you -- so you're saying that you have direct evidence and direct affidavits in your possession 19 that are going to come to light and show that this 20 21 election was fraudulent and stolen; is that what 2.2 I've heard? SIDNEY POWELL: Yes, absolutely. And we 23 24 have evidence from computer experts and 25 mathematical experts and statisticians, you don't

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

just add 350,000 Biden votes all of the sudden at three o'clock in the morning. That's like flipping a coin 350,000 times, and it always lands on heads. It doesn't happen. It's a mathematical and statistical impossibility. JOHN FREDERICKS: So in your judgment and the research you've done and what you filed, how did they manufacture these 350,000 votes for Biden in the middle of the night? SIDNEY POWELL: Well, they can just literally make up a number and inject it into the system. JOHN FREDERICKS: Huh. SIDNEY POWELL: But they also had the backup plan of the mail-in ballots or the mail-out ballots, a friend calls them, because they're just -- you know, indiscriminately mailed out by the hundreds of thousands to people. And they also had counterfeit ballots. So we have one instance where we've got this big stack of machine-generated ballots with the circle filled in perfectly just for Biden; and the techs could take stacks of those and just repeatedly run them through the machine to -- to document the backup.

```
1
           But the key -- when the algorithm broke,
 2
     when there were so many hundreds of thousands of
 3
     Trump votes at like two o'clock in the morning --
 4
     remember when all the networks suddenly stopped --
 5
           JOHN FREDERICKS:
                             Uh-huh.
           SIDNEY POWELL: -- tallying electoral votes
 6
 7
     or calling states --
 8
           JOHN FREDERICKS: Uh-huh.
 9
           SIDNEY POWELL: -- no matter --
10
           JOHN FREDERICKS: Uh-huh.
11
           SIDNEY POWELL: -- you could have 99
12
     percent of North Carolina in, and they wouldn't
13
     call it for --
           JOHN FREDERICKS: Uh-huh.
14
15
           SIDNEY POWELL: -- for President Trump,
16
     which was absolutely ridiculous; yet, as soon as
17
     the polls closed in California, they call it for
18
     Biden.
19
           JOHN FREDERICKS: Uh-huh.
           SIDNEY POWELL: We think even California
20
21
     might very well have gone for Trump.
2.2
           JOHN FREDERICKS: Uh-huh.
23
           SIDNEY POWELL: And they've been doing this
     gradually to us over the years. The states
24
25
     they're saying are blue are not blue at all.
```

1 JOHN FREDERICKS: Let's get to the truck in 2 Pennsylvania. We had Phil Kline on a little bit 3 earlier, and he said that they've got evidence -they've got -- you've an affidavit and a 4 5 whistleblower who said they drove a truck, a tractor trailer, from Bethpage, New York, to 6 7 Pennsylvania at 3:00 in the morning, dropped it off and there were 280,000 ballots in there; where 8 9 did those ballots come from, where's the truck, 10 why hasn't it been impounded, what -- are there 11 cameras, GPS? The driver said this; how did 12 ballots get from Bethpage, New York to 13 Pennsylvania? 14 SIDNEY POWELL: Well, I would guess they 15 had, you know, massive quantifies of the 16 counterfeit ballots or the pre-filled out fake 17 ballots stored in different parts of the country to send them where they were needed in the middle 18 19 of the night to backfill the system. And -- and they just -- the reason they all 20 21 had to stop counting was because they weren't 22 expecting the overwhelming -- I mean, we're 23 talking like 800,000 votes or 900,000 votes that 24 Trump had legitimately that they then had to 25 backfill in the system to try to cover for it with

1 Biden. And that's why those states had to stop 2 counting. 3 Every state that stopped counting is a -is a massive indicator of fraud. But I'm also 4 5 saying that it went far beyond all the states that had to stop counting. The ones that had to stop 6 counting, it was -- it was -- the Trump landslide was so overwhelming that it broke the algorithm. 8 9 JOHN FREDERICKS: Unbelievable. 10 SIDNEY POWELL: And they had to stop and 11 they had to backfill with fake votes and 12 counterfeit ballots. 13 JOHN FREDERICKS: What about yesterday you 14 said at the rally in Alpharetta City -- Powell 15 thus, by the way, has filed lawsuits in a number 16 of states, most recently Arizona -- by the way, 17 Kelli Ward, the Republican Party Chairman of 18 Arizona will be us, we understand, at the nine 19 o'clock hour today. Sidney Powell with us now. 20 At the rally yesterday Sid- -- Sidney, you 21 said that you uncovered evidence of -- of 2.2 counterfeit ballots being shipped in -- into the 23 U.S. from Mexico. Can you elaborate on -- on 24 that, Sidney? 25 SIDNEY POWELL: Yes. We have got some

```
1
     video of counterfeit ballots being brought across
 2
     the border from Mexico; and we also have some
 3
     evidence that there was a plane load of ballots
 4
     being flown in from outside the country. And one
 5
     witness says that that has been continuing, and
     will infect the runoff elections in various
 6
 7
    places.
 8
           JOHN FREDERICKS: You've got direct
 9
     evidence that there were counterfeit ballots
10
    printed in Mexico, basically shipped to the
11
     U.S. -- over the U.S. --
12
           SIDNEY POWELL:
                           I -- I don't know where
13
     they were printed. I don't know that they were
14
     printed in Mexico, but we know they came -- some
     came across the Mexican border into Arizona.
15
16
           JOHN FREDERICKS: All right. So they --
17
     they came in from Arizona, and -- and you believe
18
     that that was part of the -- of the fraud that
19
     perpetrated in this election trying to swing it to
     Biden, is that --
20
21
                          Definitely.
           SIDNEY POWELL:
22
           JOHN FREDERICKS: -- you have -- and you
23
     have -- and you have evidence of that?
24
           SIDNEY POWELL: Yes.
25
           JOHN FREDERICKS: You've come under
```

1 criticism by a number of establishment media in 2 the last 24 hours over this really in Alpharetta. 3 I was there, by the way, and -- saying that you 4 were encouraging people not to vote in -- January 5 5th; how do you respond to that? SIDNEY POWELL: Our point was to put 6 7 pressure on the legislature, the governor, Candidates Perdue and Loeffler and, frankly, 8 9 anybody else that would want an honest election, 10 to get out and start screaming about it. 11 if we don't fix this now, when in the world are we 12 going to? How can anyone go cast a vote for 13 anyone in a runoff election on a Dominion machine 14 or any other way than a paper ballot that they 15 know is going to be counted for the person they 16 voted for? The magnitude and -- and mass of this fraud 17 18 is -- would have been incomprehensible to me eight 19 years ago. It's what we expect in third-world -third-world countries. Well, if we're going to 20 21 turn the United States into Venezuela, let's keep 2.2 voting this way, because that's exactly what is 23 happening. 24 JOHN FREDERICKS: So what you're saying is, 25 if you don't get change now, and you go down the

```
1
     same path, they're going to end up the same place.
 2
     Stacy Abrams just had another 950,000 absentee
 3
     ballots mailed out.
           So what I'm telling people is, if you don't
 4
 5
     get change, why do you think it's going to be any
 6
     different? You're going to go to bed, January 5th
     at midnight and Perdue and Loeffler are going to
 8
     be -- head big, and then you're going to wake up
 9
     and they're going to lose. It's going to be the
10
     same -- the same thing.
11
           Why -- why would it not be the same thing?
     Tell me what -- if you don't change it, what
12
13
     exactly is going to be different?
           SIDNEY POWELL: Exactly. And even if one
14
15
     of them wins, you don't know that that was the
16
     will of the people. That's the problem --
17
           JOHN FREDERICKS: Uh-huh.
18
           SIDNEY POWELL: -- because the system has
19
     been rigged.
20
           JOHN FREDERICKS: Uh-huh. Uh-huh.
21
           SIDNEY POWELL: And everybody on both sides
22
     of the aisle should be up and jumping up and down
23
     screaming about this. One of the big problems is
24
     that it -- probably a number of Republicans have
25
     benefitted from this, too.
```

1 JOHN FREDERICKS: Uh-huh. 2 SIDNEY POWELL: Just in the end of 2019, 3 Elizabeth Warren and Amy Klobuchar and -- and some 4 other Democrats were screaming about it. 5 JOHN FREDERICKS: Huh. SIDNEY POWELL: In 2003 -- or '6, Carolyn 6 7 Maloney, a democrat from New York was screaming 8 about this and tried to warn everybody not to buy 9 the machines --10 JOHN FREDERICKS: Uh-huh. 11 SIDNEY POWELL: -- and they still got 12 So we don't know who all has benefitted 13 from it, other than the powers that be, either 14 sell or -- or know or blackmail, or whatever, 15 people to -- to rig the system. 16 JOHN FREDERICKS: And so this fraud that 17 you're doing these lawsuits on, it covers mail-in 18 ballots, it covers Dominion's software, it covers 19 algorithms, it covers counterfeit ballots coming 20 in the middle of the night -- I mean, the way 21 you've outlined this, Sidney, this -- this is a 2.2 vote-fraud-election-stealing scheme on a scale 23 that nobody could have ever imagined. But I think 24 what you've said is that because Trump was winning 25 by such a large margin, that's when the wheels

```
1
     came off their plan.
                           Right? Is that --
 2
           SIDNEY POWELL:
                           Exactly.
           JOHN FREDERICKS: -- a fair way of saying
 3
 4
     it?
 5
           SIDNEY POWELL: Yes.
                                 Yes.
                                        They have done
     any number of these things for years. But it's
 6
 7
     because he won in such a humongous landslide,
 8
     probably the largest vote count in American
 9
     history --
10
           JOHN FREDERICKS: Uh-huh.
11
           SIDNEY POWELL: -- that the wheels did come
12
     off, and -- and the fraud is being exposed.
13
     -- and people have been paying more attention.
14
     You're right, Americans all over the country are
15
     absolutely fed up with the corruption in both
16
     political parties.
17
           JOHN FREDERICKS: Uh-huh.
18
           SIDNEY POWELL: And I quarantee you that --
19
     you know, it -- it's a lot of places, at all
20
     different levels of government, local, county,
     state -- wherever, and we need to demand that it
21
22
     be stopped right now.
           JOHN FREDERICKS: Well, Sidney, what I
23
24
     think you've -- you've helped do here is ignite a
25
     movement, because I've never seen more anger
```

1 amongst voters than I have seen in the past three 2 weeks here in Georgia. 3 And what you're saying is -- look, people I 4 talked to yesterday at the rally were like, hey, 5 if I'm going to vote for these two senators, I want action; you know, give me a reason to vote 6 right now, why should I? So they can just -- just 8 steal it again and I can be made a fool out of 9 again? 10 I mean, that's what people have been saying 11 since I have been here for three weeks, and it's 12 -- the politicians don't want to acknowledge it. 13 So what they do is, McConnell's office sends -- a 14 salvo to Breitbart, then does a hit piece on Lin 15 I mean, that's the way the machine works. 16 Okay. 17 SIDNEY POWELL: Oh, yeah. 18 JOHN FREDERICKS: People --19 SIDNEY POWELL: And Lin has donated hundreds of thousands of dollars to Republican 20 21 candidates. The President is -- loves him. 2.2 loves the President. I mean, that was just 23 absolutely ridiculous. We even tried to call 24 Senator McConnell last night to explain to him 25 what was going on. And instead, you know, we get

```
1
     this ridiculous hit piece in Breitbart.
 2
           JOHN FREDERICKS: Yeah.
 3
           SIDNEY POWELL: So -- just hogwash.
                                                 Ι
 4
     mean, I'm well-aware of the fact I'm going to
 5
     irritate a whole lot of people --
           JOHN FREDERICKS: Uh-huh.
 6
           SIDNEY POWELL: -- but I think they need
 8
     irritating.
 9
           JOHN FREDERICKS: Uh-huh. Well, because if
10
     not now, when? I think what you've said here, if
11
     we don't fix this now, it's just going to continue
12
     on.
13
           I mean, they figured out how to rig it, but
14
     the most compelling thing you've said is, you
15
     know, if it was a thous- -- 10,000 votes here,
16
     15,000 votes there, they've done this in the past,
17
     they -- it gets under the radar screen.
18
           But when they look at Pennsylvania and
19
     they're losing by 900,000 votes at ten o'clock at
20
     night, that's when everything went haywire.
21
     That's when ballots start getting shipped in from
22
     New York and Bethpage in trailers.
                                         That's when
23
     machines start getting manipulated. Everything
24
     goes down.
                 They lock the -- the windows in
25
     Philadelphia.
                    They lock the doors. They throw
```

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

Cory Lewandowski out, even though we had a court That's when everything -- that's when everything fell apart for them, because it -- it had to be too big to go under the radar screen. Okay. So only got a couple more minutes. What is the pathway, what is the legal pathway right now for Trump to be inaugurated, and is there one? SIDNEY POWELL: Oh, yeah. There's -there's definitely one. There -- a number of things can happen: Legislatures need to, you know, set aside any certification of the vote and choose Trump electors. That should happen in every swing state that's an issue. Every state where the machines stopped counting in the middle of the night. You realize this is the only time in America history we stopped counting on election night? Except for one county in Florida, Broward County, in Bush versus Gore? I mean, that's how -- this was the most flagrant in-your-face abject massive voter fraud in the history of the world, other than some -- a county like Venezuela with Hugo Chavez or Mongolia or -- you know, some place where they do this all the time. That's how

1 in-our-face they were about all of it. 2 Sidney, why did they stop JOHN FREDERICKS: 3 counting the ballots, what did that allow them to Because we were all there -- like -- it was 4 5 like -- it started about 1:00 or 2:00 a.m. -about 1:00 -- 1:00 to 4:00 a.m., where they just 6 7 stopped counting. I've never seen that. covered these forever. I -- I've never seen that. 8 9 Why did -- why did they do that? Why was 10 that the plan? Because it was just not in one 11 county or state, it was in all these states they 12 just stopped counting. What was the object of 13 What was -- what were they trying to do? SIDNEY POWELL: Well, they were determined 14 15 not to give Trump 270 electoral votes on election 16 That was clear from what the media was 17 doing on all the stations, including Fox. 18 I mean, they -- they were part of this, 19 too. It was like a script came out and they had 20 all agreed that they wouldn't -- no way they were going to let Trump get to 270 electoral votes on 21 2.2 election night. 23 So the states stopped counting because --24 because he had gotten so many hundreds of 25 thousands of votes, more than their algorithm

```
1
     could fix, they had to do the things like truck in
 2
     the fake ballots or stand at the machines and run
 3
     the same ballots through 50 times until they got
 4
     the X number of votes they wanted.
 5
           JOHN FREDERICKS: Wow.
                                   So they stopped
 6
     counting --
                           That's called backfilling.
           SIDNEY POWELL:
           JOHN FREDERICKS: -- the votes --
 8
 9
           SIDNEY POWELL: They had to go in and
    backfill --
10
11
           JOHN FREDERICKS: Backfill --
12
           SIDNEY POWELL: -- fraudulent votes for
13
     Biden or insert votes. We've got the -- in -- in
14
     the machine calculations from -- I think it's
15
     Michigan, where 20 minutes apart they inject,
16
     specifically, the same number of Biden votes and
17
     Trump votes at like 354,000 X-5-4 -- you know, for
18
     Biden and then 124,352 for Trump. You know, a
19
     very specific number injected into the system
20
     twice 20 minutes apart.
21
           JOHN FREDERICKS: What are the odds on that
22
     happening?
23
                           Right. It doesn't.
           SIDNEY POWELL:
24
           JOHN FREDERICKS: In- -- infinitesimal.
25
           SIDNEY POWELL: Yes.
```

1 JOHN FREDERICKS: But yet --2 SIDNEY POWELL: Nonexistent --3 JOHN FREDERICKS: -- no one -- no one wants 4 to ask a question. No media interest in it. 5 Nothing. Zero. Just don't look here, go away. Let's talk about Biden's fantasy cabinet. 6 That's the frustration. And that's what the frustration 8 you're getting from Georgia sitting -- I think you 9 saw that yesterday, 1500 people turned out; they 10 were fired up, cheering on your every word. 11 And McConnel thinks he can have -- somebody 12 do a hit piece on Lin Wood and they're going to do 13 a hit piece on you, and that's going to make it 14 all go -- go away. 15 They don't understand that people in 16 Georgia that we're talking to have had it --17 they've had it with the whole thing. And they're 18 not going to be taken for granted. 19 And what your message is, is fix it now so 20 it doesn't happen again on January 5th, because if 21 you don't fix it, the same thing is going to 22 happen, and you want action. Everybody that I've 23 talked to who said: Look, I'm not going to vote 24 on January 5th. I'm like: Well, what do 25 Republicans have to do to get you to turn out?

```
1
     They said: Action, do something, fix this, make
 2
     me heard; otherwise --
           SIDNEY POWELL: Yeah, Loeffler -- Loeffler
 3
 4
     and -- and Perdue haven't even spoken out for
 5
     President Trump on this.
           JOHN FREDERICKS: Yeah.
 6
           SIDNEY POWELL: I mean, what the hell?
           JOHN FREDERICKS: Yeah. That's -- look, I
 8
 9
     mean --
10
           SIDNEY POWELL: The -- the Republican party
11
     is nowhere to be found on this fraud issue, which
12
     leads me to think they're as complicit in it as
13
     anybody else.
14
           The American people are a hell of a lot
15
     smarter than the politicians want to give us
16
     credit for; and we are 100 percent fed up with all
17
     of them.
18
           JOHN FREDERICKS: What would be your advice
19
     to David Perdue and Kelly Loeffler right now in
20
     order to win these two seats on January the 5th,
21
     Sidney Powell?
2.2
           SIDNEY POWELL: Absolutely demand a
23
     completely new Senate race on a paper ballot that
24
     everybody can trust, and bipartisan counting of
25
     them in full transparency.
```

1 JOHN FREDERICKS: And if they did that --2 SIDNEY POWELL: And demand --3 JOHN FREDERICKS: -- they would- --4 SIDNEY POWELL: -- a special section of the There should be a downballot race on 5 legislature. 6 everything, all over from the Senate on down in 7 Georgia. 8 JOHN FREDERICKS: Uh-huh. 9 SIDNEY POWELL: There really should be. 10 And they could put it off a little longer if they 11 needed to. 12 But it is imperative to get this right. 13 And every public official in Georgia ought to be demanding it now, and every candidate who was on 14 15 that ballot -- at least the top four contenders, 16 should be demanding that now. They owe that to 17 the American people. We are entitled to a legal 18 correct voting system that we're not defrauded 19 from. 20 JOHN FREDERICKS: Sidney Powell, I want to 21 thank you for all you do. Your lawsuits, they're 2.2 gaining traction. 23 Sidney Powell saying here in the John 24 (inaudible) show, she has direct evidence of and 25 -- and affidavits that are going to be presented

1	on voter fraud in a massive way from all angles,
2	from counterfeit ballots to truckloads of phony
3	ballots coming into Pennsylvania from New York.
4	And you know, we just had Phil Kline on
5	and I I asked him about that truckload again,
6	because I mean, it's easy to track. And he
7	said: Look, they didn't know that was going to
8	Pennsylvania; they had the ballots ready to go.
9	Maybe it was going to go to Milwaukee, maybe it
10	was going to go to Florida. It we don't know.
11	All we all we do know is
12	SIDNEY POWELL: Right.
13	JOHN FREDERICKS: Trump was ahead by
14	900,000 in Pennsylvania, so they hit the panic
15	button, and that's where they went.
16	SIDNEY POWELL: Right. Yeah, they were
17	ready for this. They have been prepared for this
18	for months. They had their legal teams ready to
19	deploy, Marc Elias and the DNC are trying to
20	intervene in all of our lawsuits, as if they had
21	any right to do so, which they don't.
22	JOHN FREDERICKS: Uh-huh.
23	SIDNEY POWELL: They have been loaded for
24	bear and planned this for a long time.
25	JOHN FREDERICKS: And you you still

```
1
     believe today that on January 20th, President
 2
     Donald J. Trump is going to put his hand on the
 3
     Bible?
 4
           SIDNEY POWELL:
                           I do.
 5
           JOHN FREDERICKS:
                              Sidney Powell --
 6
           SIDNEY POWELL: The American people see
 7
     this fraud, and we are not going to put up with
 8
     it.
 9
           (End of the recording.)
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
```

1	CERTIFICATE
2	
3	I, Jackie MENTECKY, do hereby certify that
4	I was authorized to transcribe the foregoing recorded
5	proceeding, and that the transcript is a true and
6	accurate transcription of my shorthand notes to the best
7	of my ability taken while listening to the provided
8	recording.
9	
10	Dated this 4th day of January, 2021.
11	$\Lambda = \Lambda$
12	Many by V
13	(Jews A)
14	
15	
16	Jackie MENTECKY
17	
18	
19	
20	
21	
22	
23	
24	
25	

Exhibit 99

```
1
 2
 3
 4
                                 File:
     20201205 EXCLUSIVE Sidney Powell Suspects CIA In RIGGING
 5
 6
                            Elections Huckabee
 7
 8
 9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
```

1 MIKE HUCKABEE: As legal challenges 2 continue to bring light to alleged voter fraud of the 2020 election, the clock is ticking before the 3 electoral college will meet to cast their votes 4 5 for president, just nine days from now. Across the monolithic media we hear there 6 7 is no evidence; but actually, there are hundreds 8 of sworn affidavits which are, in fact, evidence. 9 My first quest says she has evidence of 10 voter fraud on the biggest scale in world history, 11 and adds that the Justice Department either needs 12 to get his act together or be cleaned out from the 13 top-down, preferably, as she says, with a firehose 14 and Clorox. 15 Here's my conversation with former federal 16 prosecutor, attorney for our General Michael 17 Flynn, and former Trump legal counsel, Sidney 18 Powell. 19 Sidney, there are so many things I want us 20 to visit about, but I need to get something sort 21 of off the table: You have been quoted as saying 22 that maybe voters shouldn't go into Georgia and 23 vote in the Senate election, and that has been a 24 very controversial position. Do you feel like that you really are asking 25

1 Georgia republicans to stay home and not vote in 2 that very critical runoff? 3 SIDNEY POWELL: No, that was completely 4 misconstrued. Our point was that the system right 5 now is corrupt, the Dominion machines cannot be relied on at all, and we want everyone, 6 7 republicans, the candidates, everyone to stand up 8 and speak out about the fraud that happened in 9 Georgia, and find a way to vote in time that 10 allows people to know that their vote is being 11 counted the way they voted it. 12 Because right now, the system is just as 13 rigged as it was four weeks ago. We can't trust 14 it. And there has to be a way to get it right so 15 that everyone who votes, and we encourage everyone 16 to vote, knows their vote is real and being 17 counted, and not shaded or have results shaved off 18 of it and given to another candidate or otherwise 19 rigged. Well, and --20 MIKE HUCKABEE: 21 And I mean, you can't SIDNEY POWELL: 22 repeat the same procedure and expect a different 23 result. 24 MIKE HUCKABEE: Well, I appreciate your 25 clarity on that, because I think you've been

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

2.2

23

24

25

vilified by some people that said that you were trying to essentially throw the election to the democrats; and I said, I don't think that's what Sidney Powell would want to do. I -- I think I know her well enough. You -- you are a rock-star lawyer, and I say that with great affection and admiration for the many things that you have done in your legal career that have been breakthrough moments. What you're dealing with right now, in looking at the election and the manner in which it was held in a lot of states, have you ever dealt with anything quite like this before and why should everyone be worried about it? Well, even the democrats SIDNEY POWELL: pointed this out years ago, I think Carolyn Maloney was the first person I saw raise any issue about it at all, and that was back in 2006, I believe, when she spoke out vehemently against it and wrote the secretary of treasury and other people, it never should have been approved by CFIUS to have the Dominion machines used in the United States at all. I mean, none of us realized -- well, I mean, I guess a few people did, like she did, and

2

3

4

5

6

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

Elizabeth Warren and Amy Klobuchar in 2019, realized that our votes were being handled on a Venezuelan-created software platform and sent out of the country to be counted again by communist nations, with complete hackability and ease of access, to almost anyone who wanted it. I mean, we've seen a video of a 15-year-old hacking in the Dominion voting machines in a span of ten minutes, and a pro can do it in less than We also identified the fact that the Smartmatic-Dominion people left VPNs wide on and unencrypted to allow access by all kinds of foreign actors the night of the election. This election was manipulated but evil nations like China, a communist party which owns 75 percent of the investment company that owns Dominion. And then be also by Iran. There were Serbian people in the system at the time. Lichtenstein -- I mean, there were hackers all over in our own election system during the election, and we know that the Dominion machines were created for the very purpose of altering the vote count to ensure the election of people like Hugo Chavez and Maduro in Venezuela. The same thing is happening here now, and

1 this isn't the first time it's happened, Mike. We 2 don't even know how many elections have been 3 rigged by virtue of the software. 4 MIKE HUCKABEE: And, Sidney, not 5 surprisingly, Dominion comes out and says these machines are absolutely foolproof, they're full of 6 7 integrity, there's nothing to see here, let's move 8 on. 9 But more surprisingly, because that's not a 10 surprise, but more surprisingly the media keeps 11 saying there is no evidence. There's no evidence. 12 You and others have shown hundreds of affidavits, 13 sworn statements, under penalty of perjury, that 14 means a person can go to prison for lying about 15 it, of people who say they saw funny business 16 going on. 17 How come we can't seem to get the media and 18 -- and even the general public interested in the 19 evidence that you have amassed and distributed? SIDNEY POWELL: Well, I think it's 20 21 extremely unsettling to know that American 22 elections have been just as rigged as elections in 23 third-world countries have been. 24 I'm sure the CIA has been involved in any 25 number of those activities. If not here, in other

```
1
     places around the world. It may have been the CIA
 2
     that created the software and programs to begin
 3
     with, and then exported them for their own use,
 4
     only to have it come back to us.
 5
           It could be that, you know, very important
 6
     powerful, extremely wealthy people, were involved
 7
     in rigging this election. It -- it's globalists'
 8
     interest.
 9
           I mean, frankly, everyone in the world,
10
     except for the millions of Americans that wanted
11
     to elect Donald Trump to clean up the swamp and
12
     drawn the swamp, want this world to continue the
13
     way it was, with them having all the power and
14
     working behind the scenes to rig elections and
15
     everything else, so that they can profit from
16
     their own nefarious activities.
                          You know, it --
17
           MIKE HUCKABEE:
18
           SIDNEY POWELL:
                           I mean, it's massive.
19
     sure the media --
20
           MIKE HUCKABEE:
                          Yeah.
           SIDNEY POWELL: -- companies are involved in
21
22
               I noticed how all the same- -- all the
     it, too.
23
     -- the same night as if they were cued at once,
24
     they stopped counting electoral votes, and the
25
     machines stopped counting in -- in the swing
```

1 states. It was all timed and planned, and 2 organized and funded. 3 MIKE HUCKABEE: It -- it sounds like a -- a 4 movie script, but we're talking about it in real 5 time. And -- and honestly, Sidney, some of the 6 7 things that you're saying, it sounds preposterous. 8 It -- it's almost -- is beyond description. 9 In the one minute that we've got left, 10 which is not enough time, but I -- but I want to 11 keep you on your schedule, you separated yourself from the official Trump campaign lawsuits, and --12 13 I think the obvious question, why? 14 SIDNEY POWELL: Because I wanted to pursue 15 the fraud wherever it goes. And at the time the 16 campaign was focussed on an entirely different 17 avenue of approach to the election issues, I knew how important the fraud was, not just to this 18 19 country, but to the world. It should -- people of both parties, of every party, every political 20 21 persuasion, should be concerned about this. As I 22 said, the democrats were, until this election. 23 So there are no telling how many 24 congressional and senate seats and even 25 governorships we've lost, Mike, because of this.

```
1
     They've been telling us the country has been
 2
     trending blue, it has not. That is an abject lie.
 3
     And we've collected the data that's going to show
 4
     that among many other things.
 5
           MIKE HUCKABEE:
                          Even though we're out of
     time, a quick answer on this one: Is it too late
 6
 7
     to change the results --
 8
           SIDNEY POWELL:
                          No, it's not too late.
 9
           MIKE HUCKABEE:
                          -- of this election --
10
     okay.
11
           SIDNEY POWELL: No, it's not too late.
                                                    The
12
     people must absolutely demand it. The electors
13
    have not been chosen yet. The fraud in Georgia is
14
    blatant. There's a video of it that's going viral
15
     where women in the -- the State Farm Arena pulled
16
     out suitcases of ballots from under the table
17
     after they lied to people about the voting being
18
     over, and needing to go home because of a -- a --
19
     a break in a water line, or something; that was a
20
          And they counted for three hours and put
21
     illegal ballots through the machine; that was more
22
     than 20,000 votes for Biden that were false
23
     fraudulent ballots. That alone flips the state of
24
     Georgia.
25
           And the fact that the Senate (inaudible)
```

```
1
     and the governors haven't risen up and demanded
 2
     that that be fixed is extremely painful and
 3
     telling.
           MIKE HUCKABEE: Well, Sidney, I've often
 4
 5
     said that if I ever get in trouble, I'm going to
     call you; and if you ever hear from me in the
 6
     middle of the night, please take the call. Would
 8
     you just make me that promise?
 9
           Thank you for being with us and -- and
10
     sharing on our show. Thank you very much.
11
           SIDNEY POWELL:
                           You're welcome. Thank you
12
     for all that you do.
13
           MIKE HUCKABEE:
                          You can keep up with Sidney
14
     Powell on Twitter, and her website
15
     SidneyPowell.com.
16
           You can also pick up Sidney's books,
17
     including her latest, called Conviction Machine,
18
     wherever books are sold.
19
           (End of the recording.)
20
21
2.2
23
24
25
```

CERTIFICATE
I, JACKIE MENTECKY, do hereby certify that
I was authorized to transcribe the foregoing recorded
proceeding, and that the transcript is a true and
accurate transcription of my shorthand notes to the best
of my ability taken while listening to the provided
recording.
Dated this 29th day of December, 2020.
$\Lambda = \Lambda$
/ man blad V &
The state of the
<i>I</i>
JACKIE MENTECKY

Exhibit 100

Case 1:21-cv-00040 Document 1-99 Filed 01/08/21 Page 2 of 2

screenshot-twitter.com-2021.01.06-14_13_49 https://twitter.com/SidneyPowell1/status/1338920555966320641?s=20 06.01.2021



Exhibit 101

Case 1:21-cv-00040 Document 1-100 Filed 01/08/21 Page 2 of 43 FlashPoint Hope is not lost

```
1
 2
 3
 4
                             File:
 5
 6
 7
     20201229 FlashPoint - Hope Is Not Lost! Featuring
 8
                    Attorney Sidney Powell
 9
10
                 (Excerpt 16:00 minutes to 59:19.)
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
```

1 REPORTER: All right. I want to bring in 2 our special guest, via telephone, Attorney Sidney 3 Powell -- attorney. Welcome to the program. 4 SIDNEY POWELL: Oh, thank you so much. I'm 5 honored to join you. Sidney, we -- we 6 MARIA BARTIROMO: Okay. 7 are looking for hope out there, and I know you can only talk about some things, and we want to 8 9 respect that. 10 But what is it you want to tell to the --11 the good people of America, the bible-toting 12 conservative Christians that are looking for 13 something to happen; give us some hope. SIDNEY POWELL: Well, I think everybody out 14 15 there listening now needs to stand up and make 16 their voices heard. I just caught a little bit of 17 the person speaking right before I came on, and I 18 agree with absolutely everything he said. 19 But I think one of the things that needs to happen immediately, and I -- I would like to see 20 21 it happen this Sunday, is for absolutely every 22 church in the country to open up, and everybody go 23 and take their masks off, if they want to or not; 24 but open the church doors and go to church 25 everywhere across this country. They cannot

1 arrest 75 million Christians. 2 REPORTER: Right. That's good. Act- --3 absolutely. 4 All right. Okay. Attorney Powell, I have a question for you: As far as President Trump 5 retaining the presidency in this whole election 6 7 debacle that's happened, what are the viable paths that we have now to see that happen? 8 9 SIDNEY POWELL: Well, there are multiple 10 cases pending in the Supreme Court that has --11 done nothing with, we have four states in play on 12 our petitions for emergency mandamus to ask the 13 Court to decertify Arizona, Michigan and Wisconsin 14 and Georgia, because of all the massive fraud 15 there. 16 We have filed documents on each of them. 17 You can go to defending the republic.org to see the 18 documents, including the exhibits and the evidence that we filed with each one of those cases. 19 Or the website Kraken, K-R-A-K-E-N, hyphen wood.com; 20 21 which is a news aggregation site that Lin Wood and 2.2 I started to try to get the truth out to people. 23 And Twitter will not even allow you to link 24 that website in a tweet, and they -- they shut it 25 down the very first night. We got 100,000

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

2.2

23

24

25

followers the very first night we set up the Twitter account for it, and told people that it was there; so they shut the Twitter down, and they shut down the -- any ability to link that website on Twitter. All right. We -- we're going to REPORTER: get that website put up there so we can make sure our viewers can see that. And -- and, of course, good that --SIDNEY POWELL: But a -- another -- another thing is to -- I think everybody needs to start getting out in front of the homes of their state legislators and making it clear in the swing states that they want those elections decertified. The electors for Biden should not be allowed to participate in the electoral college vote in any way, shape or form. We've also filed a lawsuit against Vice President Pence in his official capacity, because we want to make sure he knows, and the law is clear, that he has the authority to reject any electors at all under the 12th Amendment to the United States Constitution; that we just filed last night late in the Eastern District of Texas. Congressman Louie Gohmert is the Plaintiff, along

```
1
 2
           REPORTER:
                      Right.
 3
           SIDNEY POWELL: -- with a number of -- a --
 4
     Arizona electors for President Trump. And the
 5
     fraud everywhere is just so outrageous.
     pretty sure they ran the algorithm to flip two
 6
 7
     points of the votes from Trump to Biden almost
 8
     everywhere across the country. Certainly they did
 9
     it everywhere on Dominion.
10
           There's already a -- a published report
11
     from the Antrim County, Michigan investigation,
12
     the only place we were allowed to examine the
13
     machines, that show that that's exactly what
14
     happened. And the vote in all the Dominion areas
15
     was 5.6 percent or so higher for Biden than any
16
     other areas in the country. And that would be
17
     attributable to that algorithm.
18
           I think the algorithm may have been run on
19
     other systems, too. It's not just Dominion,
20
     because they all use the same software, and -- and
21
     can do the same things.
2.2
                      So it --
           REPORTER:
23
           SIDNEY POWELL: For states that think they
24
     are solid on --
25
           REPORTER:
                      Right.
```

1	SIDNEY POWELL: other machines may not
2	may very well not be, we just don't know. And
3	I think if they did not have something to hide,
4	they should allow the audit of any machines
5	anybody wants to audit, frankly, anywhere in the
6	country, because we're supposed to have open
7	transparent elections in this country. Federal
8	law requires that the voting records and
9	everything respecting any kind of national
10	election, all those records be kept for 22 months
11	under penalty of going to prison
12	REPORTER: Wow.
13	SIDNEY POWELL: for up to a year, and
14	being fined in a criminal prosecution. And for
15	people to have destroyed any ballots or any
16	records, that is a a one-year penalty.
17	REPORTER: Yeah, absolute
18	SIDNEY POWELL: The reason we have that is
19	because it's so important that our elections be
20	completely trustworthy and transparent. That's a
21	hallmark of the rule of law; in a free society,
22	we're supposed to be one person, one vote. One
23	citizen, one vote.
24	REPORTER: So let me ask about January 6th.
25	Everybody's talking about that's the big day, you

```
1
     know, with the Electoral College. What if things
 2
     don't get -- is that really the end of the -- the
 3
     path or is January 20th even the end of the path?
     If we discover that there's much more fraud, and
 4
 5
     it finally comes to light and we're actually ab-
     -- people actually listened to the cases; is it
 6
 7
     possible that President Trump would be back
 8
     President Trump after January 20th, or is it
 9
     really -- is that kind of our hard cut-off date?
                          Well, it -- it's definitely
10
           SIDNEY POWELL:
11
     possible, because the Supreme Court can do what it
12
     wants to do, but it gets more difficult the longer
13
     it takes.
               The President has all the authority he
14
     needs now under the executive order that was
15
     issued in 2018 on election interference from a
16
     foreign power, there's so much evidence of that,
17
     we put out a 270-page explanation of all of it.
18
     And -- and that's published now on kraken-wood.com
19
     and defendingtherepublic.org. And I think
     probably at sidneypowell.com, too; trying to make
20
21
     it as available as we can to people, so they can
22
     see all the incredible evidence of foreign
23
     interference in the election.
24
           And, in fact, the FBI and the CISA agency
25
     documented it.
```

1 REPORTER: All right. John Graves, I -- I 2 want to pitch this over to you, John. I know you 3 have a question for Sidney Powell. 4 JOHN GRAVES: Yeah. To me, Sidney, what 5 happens -- I know it gets harder and harder with each one of these, let's say that some -- on the 6 6th that what Pence does, is sends it to the two 8 chambers, they debate for two hours, and can more 9 evidence come there because the courts lack the 10 political will to let people see the evidence, can 11 one senator get the evidence out or are there 12 McConnells of the world going to crush this? 13 SIDNEY POWELL: I -- I wish I knew all the 14 answers --15 JOHN GRAVES: Yeah. 16 SIDNEY POWELL: -- to those questions. 17 There are so many different possibilities. Vice 18 President Pence should simply refuse to accept the 19 illegal electors, the electors from the states in which there was demonstrable significant fraud. 20 21 And if he does that, then it would have to go for 2.2 President Trump. 23 REPORTER: Yeah. So -- but at that point 24 it splits between the two chambers, they debate 25 for at least two hours, but if there's very few

```
1
     senators stepping forward in this case, do you
 2
     think -- because there's a lot of opinions out
 3
     there, Pence has the authority with these dueling
 4
     electors to say, look, they sent dueling electors
 5
     here, we're just going to disgualify them all,
     which immediately triggers the 12th Amendment.
 6
           Is that a possibility the way you see this
 8
     working?
 9
           SIDNEY POWELL: Well, I -- I think the
10
    possibility is that he has the actual ability to
11
     select the President himself by virtue of
12
     disregarding --
13
           JOHN GRAVES:
                         Jefferson --
14
           SIDNEY POWELL: -- the illegal electors.
                      Right.
15
           REPORTER:
                              So --
16
           JOHN GRAVES: Yeah, Jefferson did that in
17
18
           SIDNEY POWELL: And, in fact, Thomas
     Jefferson -- Thomas Jefferson did that when he
19
20
     became President. He was actually --
21
           JOHN GRAVES:
                         Exactly.
22
           SIDNEY POWELL: -- Vice President at the
23
     time, as I recall, and then counted the electoral
24
     votes --
25
           JOHN GRAVES: And Georgia was involved,
```

```
1
     actually.
 2
           SIDNEY POWELL: -- himself. Yeah.
 3
           JOHN GRAVES: That -- that is exactly
 4
     right.
 5
           REPORTER:
                      So what about Vice President
     Pence, I -- I know that on this network and
 6
 7
     Christians all around the world, especially here
 8
     in America, we're -- we're all praying for Vice
 9
     President Pence, because there's got to be an
10
     immense amount of pressure on him.
11
           Is there anything that we can -- you can
     reveal to us there with him, and where things are
12
13
     at, and what he's thinking?
14
           SIDNEY POWELL: No, I don't know what he's
15
     thinking. I was hoping that his counsel might
16
     agree to expedite our lawsuit on these very legal
17
     issues that we're discussing right now, to make it
     clear that he has that authority, and get that all
18
19
     wrapped up so that there no- -- there's no doubt
     about it on the 6th, but they've asked for longer
20
21
     to brief it.
2.2
           And right now we have a motion to expedite
23
     the briefing schedule pending in front of the
24
     Judge in Texas that has the case.
25
           I think everybody needs to pray that Vice
```

```
1
     President Pence has the strength and wisdom and
 2
     courage, because I don't see how any good
 3
     Christian could certify a fraudulent election.
     And there is so much evidence of fraud; we haven't
 4
 5
     even begun to compile all of it. It's absolutely
 6
     massive.
           We get more every day. I'm still drinking
 8
     information through a fire hose that supports
 9
     nothing but an extraordinary criminal fraud to
10
     destroy the republic of the United States of
11
     America.
               It's not about President Trump, it's
12
     about --
13
                      Right.
           REPORTER:
14
           SIDNEY POWELL: -- the future of this
15
     republic. If we can keep it, and we're on the
16
     verge of absolutely losing it right now.
17
           REPORTER:
                      So -- and -- and, you know, to
18
     the average American sitting at home watching
     tonight -- I mean, they're sitting there going:
19
20
     How much more corruption can there be?
21
           It seems like everywhere we turn, it's
22
     like, oh, my gosh, he's -- is he a good guy?
                                                    Ι
23
     thought he was a good guy; he's a bad guy.
           What do you -- what do you say to -- I
24
25
     mean, I know we're -- we're praying and we're
```

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

praying for you, Sidney. We're going to pray before you hang up tonight, for you on the phone here; but what -- is the level of corruption in our government really to this degree that we're seeing? SIDNEY POWELL: I'm afraid it is. The real (inaudible) to steal votes, and make it appear that people have engaged in free and fair elections has been around for, at least, a decade. I'm sure it was used in 2016. To some extent it's been used in particular elections in particular It's been used all around the world in other countries. I would be willing to venture a strong quess that the CIA is probably the originator of the software to begin with; and then it was sold to Venezuela and exported everywhere, and they wanted to export it and use it to control who is in power in different places. We have trillions of dollars of global wealth and -- and power and corrupt power raging against us right now, to the -- an extent we can hardly comprehend. This is the classic battle of good versus evil, freedom versus tyranny. And they've been lining their bank accounts with

2

3

4

5

6

8

9

10

11

12

13

14

15

16

17

18

19

20

21

2.2

23

24

25

billions and billions and trillions, actually, of dollars from all these global deals they've made, and the foreign aid that's been sent from the United States to other countries, and it -- all of it's gone to line the pockets of dictators and everyone else. It's -- it's hard to wrap your head around the magnitude of this problem, but that is the reality we're facing. And I will not deny that. The only way to solve a problem is to correctly identify it. This is massive. REPORTER: That's --SIDNEY POWELL: We've got to start here. The fact that our FBI and DOJ have done nothing about this tells you how deep and wide the problem They have even had reports of some of these is. instances that we're talking about -- and we're talking about hundreds of thousands of fake ballots, and tens of thousands of illegal people voting, and duplicate votes, dead people voting -you know, all manner and means of fraud pervaded this election. But the most insidious and egregious of it is the machine fraud, and the -- the mail-in ballot scam that they used to create fake ballots

```
1
     and then try to backfill in the states that
 2
     stopped counting the night of the election so that
 3
     they could try to create the illusion that Biden
 4
     won; when they know damn well he didn't.
 5
                      Right. Let me take it over to
           REPORTER:
 6
     Lance Wallnau.
           Lance, you got a -- a final question here
 8
     for Attorney Powell?
 9
           LANCE WALLNAU:
                          Yeah.
                                   I just -- I just
10
     want to say, the person you were listening to
11
     before you spoke is Mario Murillo, and he was
12
     looking for a patent to arise, but I -- I would
13
     say that you advising every church to open and
14
     everyone to take the dang mask off and show up at
15
     the homes of state legislators -- I would say
16
     you're rather patenesque.
17
           Do you feel support coming from people that
18
     are hearing you? Because that -- you're about the
19
     boldest, clearest, most courageous voice I know
     of.
          You're like a Deborah in Israel.
20
21
           Do you feel that support out there?
22
           SIDNEY POWELL: I -- I do.
                                        I do. God did
23
     not give me a spirit of fear.
24
                      That's right.
           REPORTER:
25
                           I simply don't have it.
           SIDNEY POWELL:
```

1 I'm not going to have it. And no matter how many 2 people threaten me --3 JOHN GRAVES: Awesome. SIDNEY POWELL: -- or file suits against me 4 5 or file bar grievances against me, which has all happened in the last several weeks, it is not 6 7 going to make any difference. I am going to forge I am determined to find the truth. 8 9 know it's out there. Truth is the armor of God. 10 We are entitled to it. We are entitled to be the 11 free country that God wanted us and created us to 12 And we cannot continue to allow this tyranny 13 to have another day hold on us. 14 JOHN GRAVES: Exactly. 15 SIDNEY POWELL: And I think opening the 16 churches and everybody simply going this Sunday 17 would make a massive statement to the evil powers 18 that seek to take over this country. 19 REPORTER: Amen. Well, pastors you heard 20 it you -- you heard it right there. All right. 21 We're going to let you go here, Attorney Powell, 2.2 but I wanted to say on behalf of Kenneth Copeland and Gloria Copeland, Pastor George and Terri 23 24 Pearsons; all of us here at the Victory Channel. 25 We're praying for you. We're going to pray for

```
1
     you right now.
 2
           So Father, in Jesus name, Lord we just lift
 3
     up Sidney Powell and her team, and all that she's
 4
     dealing with. Father, we give -- ask you for
 5
     strength. We ask you for a refreshing in her body
 6
     and her mind. And thank you, Lord, for her
     resolve, and her -- her -- her attitude, and her
 8
     prowess and her -- her ability to take this where
 9
     it needs to go.
10
           Father, we put our faith behind her. And,
11
     Lord, we thank you, Father, for in Jesus name.
12
     Amen.
            Amen.
           Attorney Powell, thank you so much for
13
14
     joining us. I hope we can have you back real
15
     soon.
            I know we've all enjoyed it, having you
16
            I know you're a busy lady. We'll let you
    here.
17
     go.
18
           SIDNEY POWELL:
                           Thank you so much.
19
     thank you for all the prayers. General Flynn and
20
     I felt uplifted by all of them the whole time we
21
     dealt --
22
           REPORTER:
                      Amen.
           SIDNEY POWELL: -- with his ordeal, and we
23
24
     feel it now, too.
25
           REPORTER:
                      Yes.
```

1	SIDNEY POWELL: We have to take this
2	country back for for God, and put God back in
3	this country
4	REPORTER: Amen.
5	SIDNEY POWELL: where he belongs.
6	REPORTER: That's right. Well, you've been
7	very encouraging to us.
8	SIDNEY POWELL: We got to
9	REPORTER: Thank you very much.
10	SIDNEY POWELL: Thank you all.
11	REPORTER: And God bless you.
12	SIDNEY POWELL: Have a good night.
13	REPORTER: Yeah, bless you.
14	SPEAKER: Thank you.
15	REPORTER: Okay. So there you hear, Sidney
16	Powell right here on the Victory Channel,
17	encouraging all hope is not lost, Lance.
18	You know, you can put a smile on your face.
19	It's not gone. We there's still a path a
20	path to freedom.
21	LANCE WALLNAU: I wasn't aware that I was
22	the depressing element. Thank you. I'm
23	encouraged.
24	JOHN GRAVES: You're pointing out the
25	encourage she she is I was thinking the

```
1
     same thing, Lance, she is -- she's got the spirit
 2
     of a warrior like Patton and Eisenhower. She is a
               She's like Jael, the lady who let the
 3
 4
     enemy in the tent, and as he fell asleep from
 5
     weariness, she drove a tent peg through him and
     destroyed the enemy and delivered Israel. So God,
 6
     we just continue praying for her. We pray that
 8
     same courage over Pence. We thank you for Trump,
 9
     that you've given that.
10
           SPEAKER:
                     Yeah.
11
           JOHN GRAVES: And so God, everyone
12
     listening to us, let them stay in an attitude of
13
     prayer to encourage more --
14
           SPEAKER:
                     Yeah.
15
           JOHN GRAVES: -- courage from pastors, from
16
     judges, and from politicians.
17
           REPORTER: You know, I -- she efficiently
18
     called out all the pastors in America, you -- she
19
     called you out, open the church --
20
           JOHN GRAVES: -- called them out --
21
           LANCE WALLNAU: Yeah.
22
           REPORTER: All that is great. All right.
23
           Well, we're going to pick this up right
24
     after the break. And we're going to put all those
25
     websites back up that she talked about. We'll get
```

```
1
     all those up so you can write those down, and see
 2
     it on social media.
 3
           Hey, make sure you share this -- this
     broadcast on your social media. Go to our
 4
 5
     website, make sure you take part of all the stuff
     that we have to offer you, and we'll be right back
 6
 7
     after this break.
 8
           (Advertisement.)
 9
           REPORTER: Welcome back to FlashPoint for
10
     the second half.
11
           Listen, I -- I hope you were encouraged
12
     like we were encouraged to hear Sidney Powell say
13
            Wasn't that good? I know you guys enjoyed
     that.
14
     that.
            I think -- I think Mario is ready to go out
15
     on the road with her.
16
           So, listen, I want to play this clip that
17
     happened not too long ago with the representative
     from Georgia, Marjorie Taylor Greene.
18
                                            Listen to
19
     what she had to say, this will encourage you:
           (Recording played as follows:
20
21
           Marjorie Greene: I just finished with our
22
     meetings here at the White House this afternoon.
23
     We had got a -- had a great planning session for
24
     our January 6th objection. We aren't going to let
25
     this election be stolen by Joe Biden and the
```

```
1
     Democrats. President Trump won by a landslide.
     Call your House reps. Call your Senators from
 2
 3
     your states.
                   We've got to make sure they're on
 4
     board and we already have a lot of people engaged.
 5
     Okay. Stay tuned.
 6
           (End of playback.)
           REPORTER:
                      There you go stay tuned.
 8
     Listen, I -- there's -- there's been a shift in
 9
     this program, not that we were utterly depressed
10
     when we started. I know I pick on Lance, but he
11
     wasn't depressed.
12
           But, listen, there's a shift, you should be
13
     encouraged, this thing can still turn around.
14
     Don't give up hope, keep the faith. I can hear
15
     Brother Copeland behind me going: Have faith in
16
     God.
17
           That's what exactly what you need to do.
18
           SPEAKER:
                     Yes.
19
           REPORTER: We're going to have faith in
20
     God.
21
                       John, I want to ask you, you
           All right.
22
     know, when you heard Sidney and also represent
23
     Repre- -- Representative Greene there, there's --
24
     there's --
25
           JOHN GRAVES:
                         Yeah.
```

2

3

4

5

6

8

9

10

11

12

13

14

15

16

17

18

19

20

21

2.2

23

24

25

REPORTER: -- it's the part we don't ever see, this is what's so hard for those of us conservative believers that we're -- we're looking for anything for hope, and because of the mainstream media, we're just not getting any hope out there. JOHN GRAVES: Yeah. Yeah, and the -- and the phrase to me is put your hope in God, it is helpful when we see some evidence, but faith by definition is having belief that God is going to do something, even when we can't see it. think what is incredible about your program, Lance and Mario, encouraging people is -- is that so many people don't have any good news. And so David fed himself on God's faithfulness, and when they see little things like this, it encourages faith, I think. SPEAKER: Yeah, amen. JOHN GRAVES: So we all need it. We all need to encourage ourselves. It's the Galatians 6 It's the Hebrews 12. Your weak hands and your feeble knees, strengthen them. David Psalm -- well, First Samuel 36, he strengthened himself in the Lord. So I would encourage everybody listening to us, encourage yourself in the Lord,

```
encourage other people --
 1
 2
           SPEAKER:
                     Yeah.
 3
           JOHN GRAVES: -- and do not give up.
                                                  It is
 4
     not -- it is not over. God specializes in
 5
     miracles and he specializes in making us wait
     until the last minute.
 6
           REPORTER: Yeah.
                             That's right. All right.
 8
     Lance, I know you got something to say, in effect
 9
     -- if -- and you guys need to follow Lance,
10
     there's that Lance Wallnau -- because if you're up
11
     at 2:00 a.m., you know, you never know if you
12
     might tune in and see Lance talking about Twitter
13
     tweets from Trump at 2:00 a.m.
14
           So, Lance --
15
           LANCE WALLNAU:
                           That's exactly right.
16
                      Tell me -- tell me, what do you
           REPORTER:
17
     think? Where are we at?
18
           LANCE WALLNAU: This Twitter thing is so
19
     annoying. Four tweets from the President and the
20
     -- and Twitter decided they weren't going to put
21
                They're censoring the President of the
     them out.
2.2
     United States, people.
23
           I mean, think about how crazy, the Jewish
                                    These is how
24
     people have a term meshugana.
25
     meshugana these people are, these -- these Silicon
```

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

2.2

23

24

```
Valley oligarchs, the politicians, the big -- the
big multibillionaire Wall Street cats.
against the working-class-faith people of America.
It's just we never saw it clearly.
      And then when we voted, we expected
Republicans to represent us. Now we're finding
out that they want the vote, but they don't want
to represent us.
      This is going to lead to a cleansing --
almost like a deliverance of that spirit of
control in America. You watch, there's going to
be a backlash.
      But I just got a quick word; we're heading
into that new year time, you know in a new year
time what prophets do? The prophets are all kind
of fielding and sensing what is coming in the
        And I've been talking to them lately,
Gene.
      And here's something which I concur with,
what we're hearing: We're back at that thing
we've talked about on this program, numbers 13.
We've got Joshua and Caleb saying America shall be
saved, and God's going to bring a great
deliverance. We got the ten spies that are
saying, oh, no, no, it's not possible.
```

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

You know what bothers me? What if the future of America is in the hands of the church and the church doesn't have sufficient unity, confidence, courage --SPEAKER: That's right. LANCE WALLNAU: -- or agreement to match with Louie Gohmert and Sidney Powell, and -- and Mike Flynn are putting out there. Come on, man. So I'm -- I'm saying that right now we've got to take a look at this is going to be the year of God judging, God separating, and God empowering the remnants. When Brother Copeland talked about those local churches -- well, let's see, Sidney --Attorney Powell says: Open up this Sunday. be the pastors and the churches that are willing to step by faith into the courage that is called for, that are going to cross over into the promised land spiritually, regardless of -- of what happens in Washington. And I believe we're right now in that Chapter 13 moment. SPEAKER: Yeah. LANCE WALLNAU: I see the promised land. And I'll tell you what, God's going to separate the people that believe and see it from those that

2

3

4

5

6

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

```
don't, because two went in to that land, and ten
didn't get there because God was watching how they
responded to the moment.
     REPORTER:
                Yeah, I agree. I mean, that's a
good -- that's a good word. You ought to preach
sometime.
          That's great.
      Listen, I want to -- I want to -- let's
play this clip -- we're running out of time. I
want to play this quick clip from Representative
Greene about a tweet.
                      Watch.
      It's the tweet? Okay. Let me see it.
                                             All
riaht.
       There it is. I thought it was a video,
it's not.
     All right.
                 There it is. So she writes:
Real Donald Trump deserves his day in court, and
we're definitely going to give him his day in
Congress. We have a rapidly growing of House
         January 6th challenge is on. And there
you go, #fightforTrump, call your rep, call your
senators. You've got the information right there
you need to do. Pray and petition them to
decertify, decertify, decertify, decertify.
     All right.
                 Let's move on here. I want to
-- we're going to skip down here, guys. Let's --
I want -- something came out during the last week
```

```
1
     when we weren't able to be on the air because of
 2
     the holiday, and it was the -- about -- this is
 3
     clip number six, gentlemen, the Ukraine-Joe Biden
 4
     connection.
 5
           Now you gotta read -- this is all in
     Ukrainian, so you need to -- to read the -- read
 6
 7
     the -- the captions here, and we'll be right back.
 8
     Watch.
 9
           (Ukrainian recording played.)
10
                      All right. We're going to cut
           REPORTER:
11
     the clip, it was a little short there, because I'm
12
     -- I'm sure you were getting tired of hearing it,
13
     but the -- listen, I want to go back and read a
14
     little -- reread what -- part of what he said
15
     there.
16
                     They really didn't want us to
           He says:
17
     publish what we're going to release today; what
18
     will be disclosed, evidence of withdrawal through
     financial halls of millions of dollars stolen from
19
     the Ukrainian people, laundered with the help of
20
21
     banks and laundromats in various jurisdictions --
22
     blah, blah, blah -- all transferring to the
23
     accounts of the company belonging to the Biden
24
     family.
25
           All right.
                       John, you want to speak to
```

```
I mean, now we've got the Ukrainian
 1
     that?
 2
     speaking the truth --
 3
           JOHN GRAVES:
                         Yeah.
 4
           REPORTER:
                     -- more than our own media.
 5
     what do we make of that?
                         There was a poll that came
 6
           JOHN GRAVES:
 7
     out after the election when people found out that
 8
     the mass media hid purposely the Hunter Biden
 9
     story, that 14 percent of the people who voted for
10
     Joe Biden would not have voted for him.
           This is just further evidence.
                                           There's not
11
12
     just fraud. We can talk about lawsuits all day
13
     long, but the fraud is very simple, very clean and
14
     very clear. When people in Pennsylvania --
15
     hundreds of thousands are accepting votes way
16
     after the election, it violates the state law,
     which violates the constitution.
17
                                        This is not
18
     complicated.
19
           This Ukrainian -- Hunter's laptop, and all
     the other stuff that was hidden, is just part of
20
21
     the underlying fraud. If I were to stop you at an
2.2
     election and threaten you, that would literally be
23
     interfering that would be fraudulent, it would be
24
     stopping an election.
           When the media is withholding evidence that
25
```

```
1
     changes the minds of the people who are voting,
 2
     they're interfering with elections.
 3
     later it should be dealt with. We just heard from
 4
     Sidney Powell; she's a street fighter. We have a
 5
     President who's a street fighter. Mario is a
 6
     street preacher; he knows there's a different
 7
     tactic that you use when you go to these kind of
 8
              That's what we need right now, is street
 9
     fighters in those pulpits. Street preachers that
10
     will speak the truth, even when it's unpopular.
11
           REPORTER:
                      Yeah, that's right.
                                            I --
12
                         I'm just speaking it plain.
           JOHN GRAVES:
13
                      Yeah, you are. And -- and
           REPORTER:
14
     Mario, I think he's -- he's talking your language
     right there. In fact --
15
16
           SPEAKER:
                     Yeah.
17
           REPORTER: -- I think you were right, you
18
     nailed it when they're patenesque with Sidney
19
     Powell, she really is coming after it.
           MARIO MURILLO: You know, I -- I feel like
20
21
     we've got something backwards in the Christian
2.2
     movement in America, that we want God to comfort
23
     us right now. This isn't a moment to be
24
     comforted.
25
                      That's right.
           REPORTER:
                                     It's --
```

1 JOHN GRAVES: This -- this is not a moment 2 for you to be emotionally saved to hope that 3 everything comes out. This is God trying to put a 4 fight in you, to put a fire in you, according to 5 Nehemiah 4:14 where he told the people, he said: Listen, don't listen to your enemies, don't listen 6 7 to their threats, but fight for your family; and remember the Lord God who is awesome. 8 9 And I know it's an uncomfortable message, 10 I know it is. But I want to tell you, folks. 11 people told me the way you're preaching right now, 12 Mario, it's so straight, nobody's going to get 13 saved because they're going to think you're a pol--- a political activist. We've got more drug 14 15 addicts and gangsters getting saved now than we've 16 ever seen, because they intuitively understand 17 when someone is telling the truth. 18 And I'm telling you right now the truth; we 19 flip this. We don't need Ovaltine. We don't need 20 consolation. We need the pilot light to be turned 21 into flame --22 REPORTER: Right. Right. 23 MARIO MURILLO: -- and for everybody to 24 activate and do their righteous duty right now. 25 Yeah, Lance, you agree with REPORTER:

1 that? I mean, I -- I like what Mario is saying. 2 JOHN GRAVES: No, total- -- totally. 3 -- and it's time that the prophets and the 4 prophetic actually got ahead of the curve here, 5 because we've been saying for a while that what Obama wants to do is remove Biden and get Harris. 6 7 Harris couldn't get elected on her own. 8 the Sorosean-Biden-Eric Holder-axel-rod pick. 9 she was made vice President and -- because she 10 could never get elected as President. 11 So now they're going to remove Biden. 12 were these stories all suppressed, by the way? 13 Why was it you couldn't hear this in any media? And suddenly there's an agreement that it's going 14 15 to come out -- that quy looks so suspicious to me. 16 I mean, he's telling the truth. He could have 17 told it during President Trump's impeachment 18 situation. The FBI could have revealed the laptop 19 during the impeachment. I say it's time we got some Elisha 20 21 anointing, and started eavesdropping on what the 2.2 CIA and the corrupt government is doing to plant 23 stories in media to manipulate people so that --24 oh, let's go get over -- you know what they want 25 They want to give Joe Biden's scalp to all to do?

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

```
the angry people over the election fraud, and put
in a smiling new female face that everybody can
gloat over.
            It's not going to work that way. I
think the prophetic is getting smart, and God's
people aren't going to be taken advantage of.
      REPORTER:
                Yeah, I agree. I think you're
absolutely right.
                   That -- that is the ultimate
qoal.
      You know, John, what we're seeing here, as
people are pushing more into what this election
has turned into -- you know, I -- I have graphics
and we can go over those on another program -- I
think we've -- there's been so much data, and
we're being deluged -- with, you know, wild
conspiracy theories to -- oh, it's done or oh it's
not or Trump's in Hawaii -- somewhere -- you know,
there's crazy stuff out there, it -- but this
really is -- we really can see something turn
around, can't we?
                   I -- I still believe it.
      JOHN GRAVES:
really do. I know it looks like a long shot in
the natural, from a legal standpoint, but remember
what Trump said in his very first debate, I'm
fighting a two-war front. Jesus fought a two-war
front. He fought demonic oppression, which I
```

2

3

4

5

6

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

```
think is the whole fraudulent thing.
                                      But then
there is a second front against those who don't
want to lose power.
                 That's right.
      REPORTER:
      JOHN GRAVES:
                    They don't have the political
courage to do the right thing, and he is.
      And so what we need to pray from Pence all
the way down -- Trump has it, Sidney has it, there
are people that have it. We need to pray that all
the way down, especially in the United States
Senate, the House state legislatures -- especially
in these six or seven swing states -- that they
have courage to do the right thing, and to fight
both fraud and evil; but also the pharisee spirit
of people who want to maintain power, and they're
just worried about the next election.
                                       They're the
ones that need pressure from the people, like
Mario said.
      REPORTER:
                 Yeah. And -- and I agree with
      And -- and this is a time, like Mario said,
for us to push in, you know, suck it up and stop
being a -- a baby Christian. You know, it's time
for the believers to rise up and act like they got
the -- the power. You know, we got the big guys
to --
```

1 JOHN GRAVES: There's a time for peace, and 2 a time for war. That's right. 3 REPORTER: That's right. And you know when 4 -- when you're in grade school, and you're playing 5 basketball, you want to get picked -- you pick the 6 tall guys first, and that's -- that's the way it was in grade school, or -- or playing on the 8 asphalt jungle there. And -- and so we've got the 9 biggest teammate. We've got the guy who's 10 winning, and is going to win and -- listen, we've 11 got to keep praying for President Trump. 12 got to pray for those in the White House. 13 JOHN GRAVES: Yes. 14 REPORTER: Listen -- and you -- you 15 correctly said it, he's fighting a war within his 16 own house at the White House, and we pray for him 17 and Melania. In fact, Mario, I think you should do that, 18 19 if you would, sir. Let's pray for President 20 Trump, Vice President Pence, Melania, and all 21 those that are dealing with what they're dealing 2.2 with right now. MARIO MURILLO: Father, in the name of 23 24 Jesus, I pray for the boldness of a lion to come 25 on Mike Pence. I pray to, oh God, because I know

2

3

4

5

6

8

9

10

11

12

13

14

15

16

17

18

19

20

21

2.2

23

24

25

his background and I know his story, that he's going to do the right thing. And I pray, oh God, that he will not consider even his own safety, but he will consider the -- the nation. Lord, I pray for President Trump that he will not allow his fear of it being self-serving for him to declare this election an in- -- interference that should by executive order be interrupted. If he needs to do what Jefferson did, help him, oh God, to do it; and disregard anyone around him that would give him inferior or human advice. And I pray, oh God, for our audience tonight. Lord, when I preach sometime I'll tell the lost, I'll say: You want God to prove to you that he's real, but God is standing there saying I want you to prove to me that you're real, that you really want to be delivered and saved. And I believe that right now God -- the word of God says that God looked for someone to stand in the gap and he was amazed that no one would do it. And right now God is searching the hearts of every individual who's watching to see if there is a remnant that will rise up and discard the compromise and the fear and become the force that God has birthed them to become in this

```
1
    hour.
            We will never see an opportunity like this
 2
     again in our life.
 3
           Help us, oh God, to seize it in the name
 4
     above every name, the name of Christ.
 5
           REPORTER:
                             And we agree with that.
                      Amen.
 6
           All right.
                       I want to put up these websites
 7
                    Those of you watching on social
     before we go.
 8
     media, they -- it looks like they've got them
 9
     there for you to see: Defendingtherepublic.org.
10
     Defendingtherepublic.org. You can see what's
11
    happening there and how to follow.
           Then there's kraken-wood --
12
13
     kraken-wood.com.
                       I think I'm going to go to that
     one, just because of the name of it. I just want
14
15
     to go to -- and I noticed, Mario, you didn't say,
16
     you know, release the Cracker Barrel. I was
17
     really proud of you.
18
           MARIO MURILLO: No.
                                No.
                                     I -- I was
19
     honoring Sidney tonight and --
20
           LANCE WALLNAU: Good --
21
           REPORTER:
                       Yes.
22
           LANCE WALLNAU: Good behavior tonight.
23
           REPORTER:
                      And, of course,
24
     sidneypowell.com; you can go there and stay in
25
     touch.
```

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

And keep her in your prayers. Listen, you got to -- you got to pray and keep that up. as -- again, we're going to play this clip again about what's coming up January 6 in our nation's capital. Listen, if you haven't made your reservations, make your reservations, get your flights, drive in, be there; you want to be there January 6 from 10:00 a.m. to 5:00 p.m., your President has asked you to join him there for the wild protest -- wildprotests.com. We're going to play this video. We'll be right back. (Video played as follows: Speaker: We will not bend. We will not break. We will not heal. We will never give in. We will never give up. And we will never back We will never ever surrender, because we are Americans, and our hearts bleed red, white and blue. Stop the steal. Stop the steal. Stop the steal. (End of playback.) That's right, stop the steal, REPORTER: and we agree with that. The steal is stopped in Jesus name. All right. Before we comment in our last

1 round here, I want to play an encouraging clip from Brother Copeland, and watch this, talking 2 3 about the victory. Watch. 4 (Video played as follows: 5 Brother Copeland: Take no thought concerning losing, cast that thought down. 6 7 take it by saying it. Let it die. Let that --8 that thought die unborn. And keep victory in your 9 mouth, for this is the victory that overcometh the 10 This is the victory that overcometh Covidworld. 11 -- Covid-19. This is the victory that overcometh the attempt to steal this election. 12 This is the 13 victory that overcomes the world. Even our faith. Even our faith. 14 REPORTER: Amen. Amen. 15 First John 5:4, you're going to hear that a lot 16 around here. First John 5:4, this is the victory 17 that overcomes the world, even our faith. 18 All right. Gentlemen, we got three 19 minutes. Okay. Mario, I'll let you go first. Let you first up, final thoughts. 20 MARIO MURILLO: Well, one thing I want to 21 22 tell you is that Lance Wallnau is a gift to the 23 body of Christ that is incredibly important in 24 this hour, because God has used him to cross over 25 into other arenas to speak.

1 And I felt in this moment that I needed to 2 just say this, that God's hand of protection and 3 promotion is on this man. 4 REPORTER: Amen. 5 MARIO MURILLO: And that he has a special ability to decode what's going on right now. 6 7 I'm a soul winner, and I want to win souls. to be honest with you, I'm only here because I --8 9 I want to get back to winning souls. And the only 10 way I can do it is in a free country. 11 REPORTER: That's right. 12 MARIO MURILLO: And that's why I'm doing 13 this. 14 LANCE WALLNAU: Hallelujah. 15 MARIO MURILLO: But I wanted to make it 16 clear that my visit in these shows is all about 17 one thing, that I believe that God has put 18 together in this FlashPoint program a unique voice 19 in America, and that there is a unique voice in --20 in Lance Wallnau -- and I'm not trying to just 21 flatter the man, I'm praying for him, because he's 2.2 on the frontline. 23 I'm glad for everyone that's with us 24 tonight, it's an honor to be with every one of 25 you, but I believe that we have to -- we have to

```
1
     take inventory of the opportunity that we are
 2
     standing in right now.
                             It's once in a lifetime.
 3
           REPORTER:
                      Yeah.
                             Amen.
                                    I -- I actually
 4
     agree with that, Lance. You don't have to say
 5
     anything. I actually agree with that.
     John Graves, go ahead.
 6
                         To me it's a -- it's
           JOHN GRAVES:
 8
     decertify, pray for Pence to have the courage,
 9
     like Lance talked about with Caleb and Joshua --
10
     remember when he went back, I was reading through
11
     the bible, and I got to the 12th chapter where he
12
     defeated 31 different kings and listed every
13
     single one of them. And when he went back, he
14
     didn't have 10 weak spies.
15
           And I love how Sidney said it, I -- I'm --
16
     I'm not denying the truth, here's the truth, Caleb
17
     and Joshua didn't come back and say we're denying
18
     the truth, they just said God's bigger, that --
19
     yeah, there's giants in the land, we can do this.
20
           So -- so to me the courage meant to the
21
     body of Christ is faith, it can still move this,
2.2
     don't stop praying. If God spoke to you, keep
23
     speaking it.
24
                      Yeah.
                             Amen.
                                    All right.
                                                 Lance?
           REPORTER:
25
           LANCE WALLNAU: Yeah. I'm wondering, do
```

```
1
     you have me going last because last time when I
 2
     went first I talked too long, remember that?
 3
           REPORTER:
                      I'm trying to find that sweet
 4
     spot -- I'm trying to find that sweet spot for
 5
     you.
 6
           LANCE WALLNAU:
                           I know what you're up to.
 7
     I know what you're up to.
 8
           JOHN GRAVES: -- the best for the end,
 9
     Lance. The best for the end.
10
                          Okay. Well, here -- here's
           LANCE WALLNAU:
11
     the verse when John when -- when Caleb and -- and
12
     Joshua were trying to persuade their -- their
13
     generation, remember what they said, they said:
14
     If the Lord delights in us he's going to bring us
15
     into the land, he'll give it to us, only don't
16
     rebel against the Lord, neither fear the people of
17
     the land, because they're bred for us.
18
           I would love to hear at some point -- and
19
     not on this broadcast, but in the future, what you
20
     guys think about that statement, they're bred for
21
          It literally means that what you overcome
22
     nourishes you. And God's calling us to grow in
23
     the battle, not run from it.
24
           REPORTER:
                      Amen.
                             Good.
                                    Good.
                                           All right.
25
     So there -- there you've got it, to rise up church
```

```
1
     believers, pastors, open your church, go to church
 2
     this Sunday, pray for the President, pray for Vice
 3
     President Pence.
           Thank you Kenneth Copeland Ministries for
 4
     allowing this program to be here. Thank you,
 5
 6
     gentlemen, for joining me. And, of course,
 7
     Attorney Sidney Powell. So much more coming up;
 8
     you don't want to miss this Thursday, New Year's
 9
     Eve, right here on the Victory Channel. We'll see
10
     you then.
11
           (End of the recording.)
12
13
14
15
16
17
18
19
20
21
22
23
24
25
```

1	CERTIFICATE						
2							
3	I, Jackie Mentecky, Transcriptionist/Court						
4	Reporter, do hereby certify that I was authorized to						
5	transcribe the foregoing recorded proceeding, and that						
6	the transcript is a true and accurate transcription of my						
7	shorthand notes to the best of my ability taken while						
8	listening to the provided recording.						
9							
10	Dated this 3rd day of January, 2020.						
11	$\Lambda = \Lambda$						
12	God Miles						
13							
14							
15							
16	Jackie Mentecky						
17							
18							
19							
20							
21							
22							
23							
24							
25							

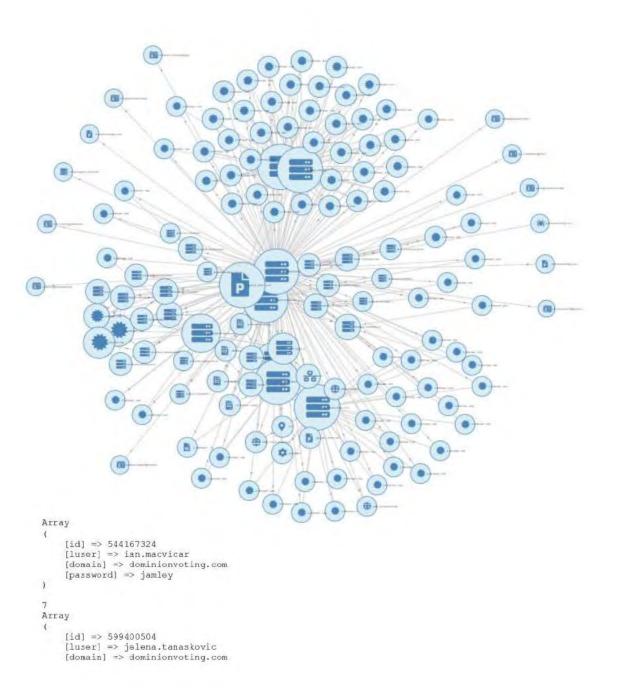
Exhibit 102

Foreign Ties and Vulnerabilities

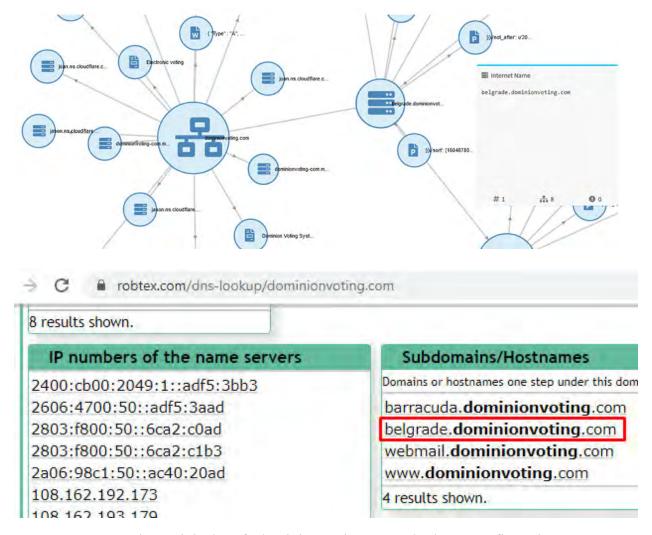
2 001					
Pursuant to 28	U.S.C Section 174	6. I.	I, make the	following	declaration.

Declaration of

- 1. I am over the age of 21 years and I am under no legal disability, which would prevent me from giving this declaration.
- 2. I served in the US Army with 2 combat deployments and left the Army under Honorable conditions. After leaving the Army I went to college and worked under a mentorship with the Late Professor Kevin Henson for 4 years after leaving the Army. In 2017 I began working at Allied Special operations group (ASOG) in Charge of Cyber Operations under the mentorship of Kevin until his passing in 2019. While at ASOG I began investigating election fraud prior to the 2018 Midterms and worked on multiple cases from Texas to Kentucky researching election fraud and vulnerabilities of the election system. It was during this time that Russ Ramsland and I notified many of these vulnerabilities from the FBI to elected officials.
- 3. I am a US citizen and I reside at **Dallas**, **TX** location in the United States of America.
- 4. Whereas the Dominion and Edison Research systems exist in the internet of things, and whereas this makes the network connections between the Dominion, Edison Research and related network nodes available for scanning,
- 5. And whereas Edison Research's primary job is to report the tabulation of the count of the ballot information as received from the tabulation software, to provide to Decision HQ for election results,
- 6. And whereas Spiderfoot and Robtex are industry standard digital forensic tools for evaluation network security and infrastructure, these tools were used to conduct public security scans of the aforementioned Dominion and Edison Research systems,
- 7. A public network scan of Dominionvoting.com on 2020-11-08 revealed the following interrelationships and revealed 13 unencrypted passwords for dominion employees, and 75 hashed passwords available in TOR nodes:



8. The same public scan also showed a direct connection to the group in Belgrade as highlighted below:



9. A cursory search on LinkedIn of "dominion voting" on 11/19/2020 confirms the numerous employees in Serbia:



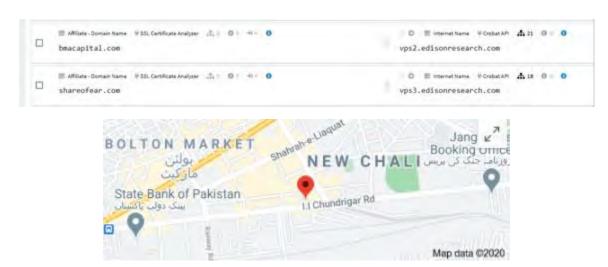
10. An additional search of Edison Research on 2020-11-08 showed that Edison Research has an Iranian server seen here:



Inputting the Iranian IP into Robtex confirms the direct connection into the "edisonresearch" host from the perspective of the Iranian domain also. This means that it is not possible that the connection was a unidirectional reference.



A deeper search of the ownership of Edison Research "edisonresearch.com" shows a connection to BMA Capital Management, where shareofear.com and bmacapital.com are both connected to edisonresearch.com via a VPS or Virtual Private Server, as denoted by the "vps" at the start of the internet name:

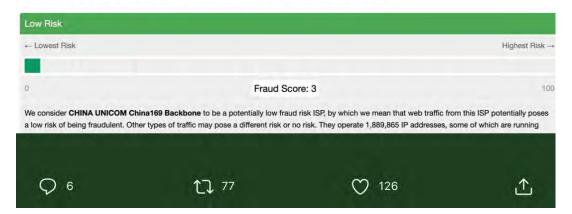


There are also many more examples, including access of the network from China. The records of China accessing the server are reliable.





CHINA UNICOM China169 Backbone - Fraud Risk



Domain Name: dominionvotingsystems.com

Registry Domain ID: 2530599738_DOMAIN_COM-VRSN

Registrar WHOIS Server: whois godaddy.com Registrar URL: http://www.godaddy.com Updated Date: 2020-05-26T15:48:58Z Creation Date: 2020-05-26T15:48:57Z

Registrar Registration Expiration Date: 2021-05-26T15:48:57Z

Registrar: GoDaddy.com, LLC Registrar IANA ID: 146

Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505

Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited

Registrant Organization:

Registrant State/Province: Hunan

Registrant Country: CN

Registrant Email: Select Contact Domain Holder link at

https://www.godaddy.com/whois/results.aspx?domain=dominionvotingsystems.com

Admin Email: Select Contact Domain Holder link at

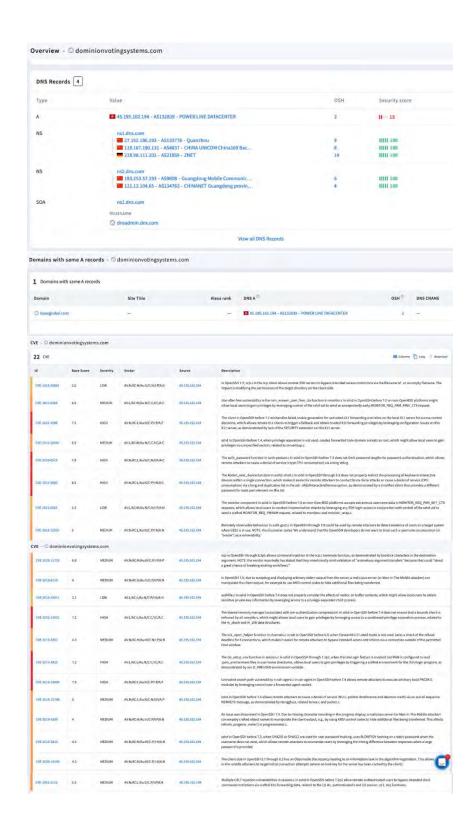
https://www.godaddy.com/whois/results.aspx?domain=dominionvotingsystems.com

Tech Email: Select Contact Domain Holder link at

https://www.godaddy.com/whois/results.aspx?domain=dominionvotingsystems.com

Name Server: NS1.DNS.COM Name Server: NS2.DNS.COM DNSSEC: unsigned

Case 1:21-cv-00317-DCLC-CHS Document 22-7 Filed 01/20/22 Page 508 of 591 PageID



11. BMA Capital Management is known as a company that provides Iran access to capital markets with direct links publicly discoverable on LinkedIn (found via google on 11/19/2020):

www.linkedin.com > muhammad-talha-a0759660

Muhammad Talha - BMA Capital Management Limited

Manager, Money Market & Fixed Income at BMA Capital Management Limited. BMA Capital ...

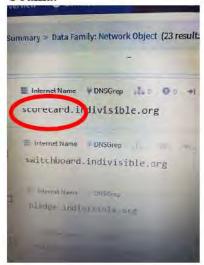
Manager-FMR at Pak Iran Joint Investment Company. Pakistan.

Pakistan - Manager, Money Market & Fixed Income - BMA Capital Management Limited

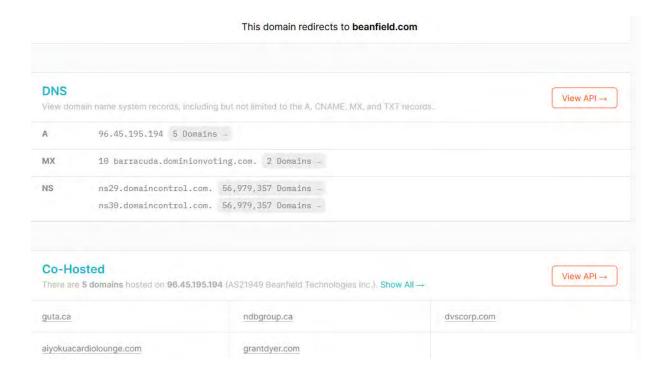
The same Robtex search confirms the Iranian address is tied to the server in the Netherlands, which correlates to known OSINT of Iranian use of the Netherlands as a remote server (See Advanced Persistent Threats: APT33 and APT34):



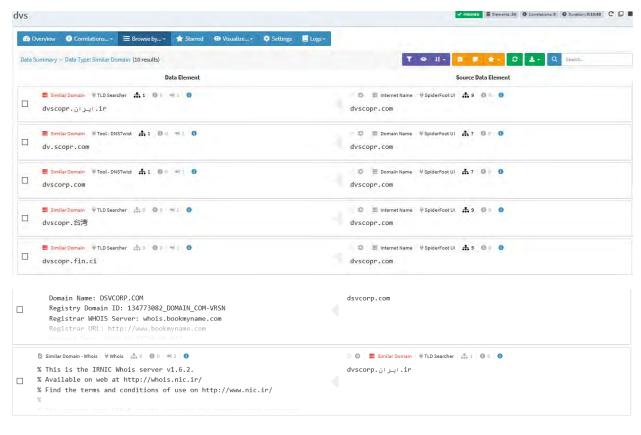
12. A search of the indivisible.org network showed a subdomain which evidences the existence of scorecard software in use as part of the Indivisible (formerly ACORN) political group for Obama:

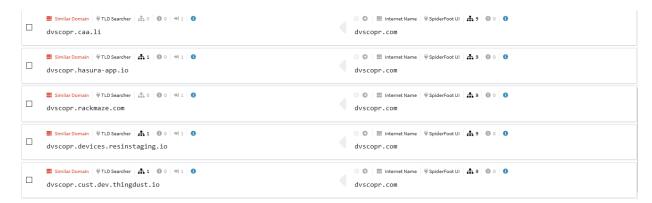


- 13. Each of the tabulation software companies have their own central reporting "affiliate".
 Edison Research is the affiliate for Dominion.
- 14. Beanfield.com out of Canada shows the connections via co-hosting related sites, including dvscorp.com:



This Dominion partner domain "dvscorp" also includes an auto discovery feature, where new innetwork devices automatically connect to the system. The following diagram shows some of the dvscorp.com mappings, which mimic the infrastructure for Dominion:





The above diagram shows how these domains also show the connection to Iran and other places, including the following Chinese domain, highlighted below:



- 15. The auto discovery feature allows programmers to access any system while it is connected to the internet once it's a part of the constellation of devices (see original Spiderfoot graph).
- 16. Dominion Voting Systems Corporation in 2019 sold a number of their patents to China (via HSBC Bank in Canada):

Assignment details for assignee "HSBC BANK CANADA, AS COLLATERAL AGENT"

Assignments (1 total)

Reel/frame	Execution date	Date	Pages
050500/0236	Sep 25, 2019	recorded	7
		Sep 26,	
		2019	
Con	veyance		
SECURITY	AGREEMENT		
Assignors	Correspond	ent	Attorney docke
DOMINION VOTING SYSTEMS CORPORATION	CHAPMAN & CUTLE		
	1270 AVENUE (AMERICAS, 30TH		
	ATTN: SOREN SCHW		
	NEW YORK, NY 1002	.0	
Assignee			
HSBC BANK CANADA, AS COLLATERAL AGENT			
4TH FLOOR, 70 YORK STREET			
TORONTO M5J 1S9			

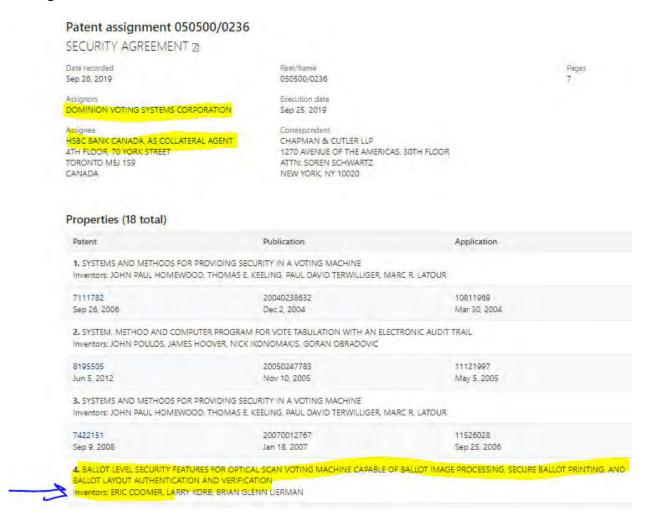
	Properties (18)			
Patent	Publication	Application	PCT	International registration
8844813	20130306724	13476836		
8913787	20130301873	13470091		
9202113	20150071501	14539684		
8195505	20050247783	11121997		
9870666	20120232963	13463536		
9710988	20120259680	13525187		
9870667	20120259681	13525208		
7111782	20040238632	10811969		
7422151	20070012767	11526028		
D599131		29324281		

View all

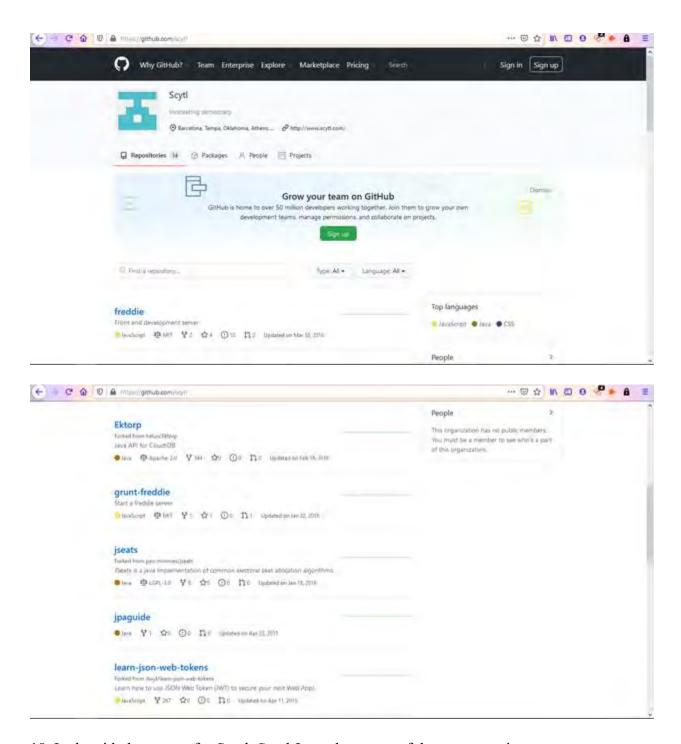
This searchable database contains all recorded Patent Assignment information from August 1980 to the present.

When the USPTO receives relevant information for its assignment database, the USPTO puts the information in the public record and does not verify the validity of the information. Recordation is a ministerial function—the USPTO neither makes a determination of the legality of the transaction nor the right of the submitting party to take the action.

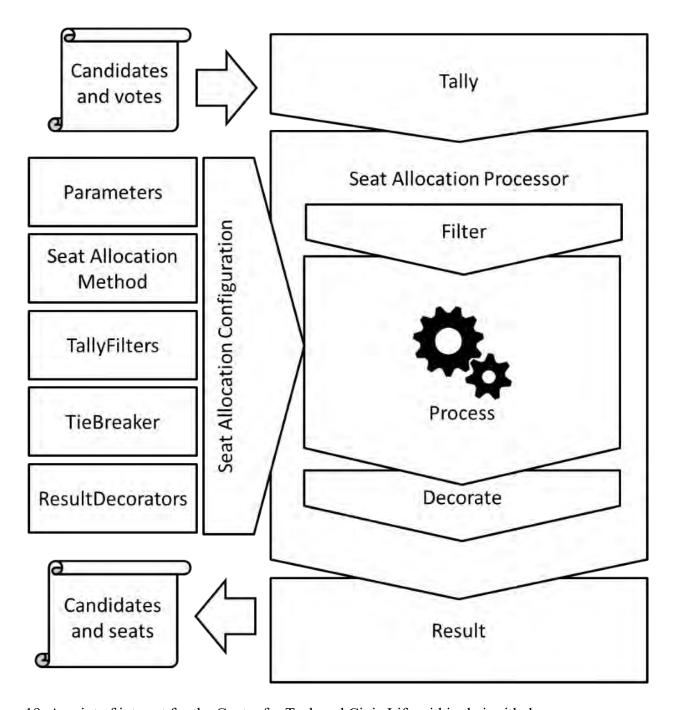
Release 2.0.0 | Release Notes | Send Feedback | Legacy Patent Assignment Search | Legacy Trademark Assignment Search Of particular interest is a section of the document showing aspects of the nature of the patents dealing with authentication:



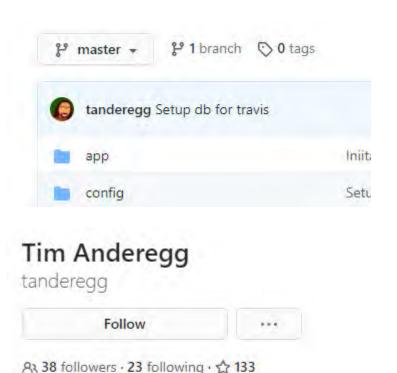
17. Smartmatic creates the backbone (like the cloud). CTCL is responsible for the security within the election system.



18. In the github account for Scytl, Scytl Jseats has some of the programming necessary to support a much broader set of election types, including a decorator process where the data is smoothed, see the following diagram provided in their source code:



19. A point of interest for the Center for Tech and Civic Life within their github page (https://github.com/ctcl) is that one of the programmers for Edison Research holds a government position. The Bipcoop repo shows tanderegg as one of the developers, and he works at the Consumer Financial Protection Bureau:



20. As seen in included document titled

Consumer Financial Protection Bureau

"AA20-304A-

Washington DC

Iranian_Advanced_Persistent_Threat_Actor_Identified_Obtaining_Voter_Registration_Data "that was authored by the Cybersecurity & Infrastructure Security Agency (CISA) with a Product ID of AA20-304A on a specified date of October 30, 2020, CISA and the FBI reports that Iranian APT teams were seen using ACUTENIX, a website scanning software, to find vulnerabilities within Election company websites, confirmed to be used by the Iranian APT teams buy seized cloud storage that I had personally captured and reported to higher authorities. These scanning behaviors showed that foreign agents of aggressor nations had access to US voter lists, and had done so recently.

21. In my professional opinion, this affidavit presents unambiguous evidence that Dominion Voter Systems and Edison Research have been accessible and were certainly compromised by rogue actors, such as Iran and China. By using servers and employees connected with rogue actors and hostile foreign influences combined with numerous easily discoverable leaked credentials, these organizations neglectfully allowed foreign adversaries to access data

and intentionally provided access to their infrastructure in order to monitor and manipulate elections, including the most recent one in 2020. This represents a complete failure of their duty to provide basic cyber security. This is not a technological issue, but rather a governance and basic security issue: if it is not corrected, future elections in the United States and beyond will not be secure and citizens will not have confidence in the results.

I declare under penalty of perjury that the forgoing is true and correct tφ the best of my

knowledge. Executed this December 16th, 2020.

Exhibit 103

Case 1:21-cv-00040 Document 1-102 Filed 01/08/21 Page 2 of 14 John Catsmatidis Interview with Sidney Powell January 03, 2021

				-			
1							
2							
3							
4			Fil	le:			
5							
6	John	Catsimatidis	interview	with	Sidney	Powell	1-3-21.
7							
8							
9							
10							
11							
12							
13							
14							
15							
16							
17							
18							
19							
20							
21							
22							
23							
24							
25							

```
1
           JOHN CATSIMATIDIS: Good morning, America.
 2
     This is The Cats Roundtable.
                                   John Catsimatidis
 3
     here. It's Sunday morning.
 4
           Well, it's a new year. Well, what's going
 5
         What's going on in Washington? What's going
 6
     on in Georgia?
           Well, we have with us one of the smartest
 8
     ladies I know; we have Sidney Powell.
 9
           And good morning, Ms. Powell. How are you?
10
           SIDNEY POWELL: Good Morning, John.
11
     you so much. I'm fine. And Happy New Year.
12
           JOHN CATSIMATIDIS: Happy New Year.
13
     hope it's a -- we need a better year than 2020.
14
     Definitely.
15
           SIDNEY POWELL: We certainly do. We need a
16
     year we're free, and ring (inaudible) loud, an
17
     individual, once they're held accountable for
18
     their egregious crimes against this country --
19
           JOHN CATSIMATIDIS: And -- and --
20
           SIDNEY POWELL: -- and the President, and --
           JOHN CATSIMATIDIS: It -- it's horrible.
21
2.2
     Like I can't believe what's going on. And, you
23
     know, some of my friends that say -- look at me
24
     and say I'm crazy to even think it; I said you're
25
     -- you're being naive.
```

1 Give us an update what you think is going 2 on in Georgia, what you think is going on in 3 Washington; is there going to be any justice in 4 the new year? 5 SIDNEY POWELL: Well, I -- I keep praying, and -- and there must be, John, or we have a 6 7 complete collapse of this republic and the rule of 8 law. 9 I've been very concerned about it for 10 several years, that concern has only increased. 11 The presidency of Donald Trump and the fact that 12 he's an outsider and has taken steps to put China 13 in their place and to eliminate all their control 14 over the country and different people has, 15 obviously, revealed so much corruption, it's 16 beyond comprehension. But it's there and it's real. If we don't 17 18 fix it right now, I don't know when we would have another chance, because it will -- it will double 19 if it's allowed to survive this election. 20 21 the most fraudulent election in the history of the 22 It's just -- it's so ' well documented 23 and so observable. Most people saw it start 24 election night. They -- they saw it with their 25 own eyes. Votes don't disappear from one

1 candidate and go to the other; yet, people saw 2 that happen. 3 We know it happened. We have election 4 machines and -- and a report done on those by 5 experts that show that votes were flipped from Trump to Biden, and how the votes were 6 7 manipulated, according to an algorithm. -- a whole separate issue from hundreds of 8 9 thousands of fraudulent ballots being created, 10 and -- and printed for Biden only and injected 11 into the system when all the voting stopped across 12 multiple states; which has never happened before 13 in the history of the country. 14 One time -- one election night voting 15 stopped in Broward County, Florida, and -- and 16 that was a major disaster and caused all kinds of 17 problems. Voting does not stop in this country. 18 It's supposed to go continuously. And the only 19 reason they stopped it was Trump was so many 20 hundreds of thousands of votes ahead, if it had 21 been a legitimate election they would have called 2.2 for him then. But instead, they brought in boxes 23 and boxes of fake ballots and ran them through the 24 Dominion machines to count them for Biden. 25 And we know, for example, in -- in Fulton

1 County, Georgia, that they had a 93-percent, I 2 think it was, what they call adjudication rate; that means the machines didn't count those ballots 3 at all, they were kicked into a file for a human 4 5 being to decide in a matter of minutes where those hundreds of thousands of votes went. 6 And so they trashed some for Trump, they just assigned them to 8 Biden or to a third-party candidate, and then to 9 Biden, and it was all manner of means of fraud in 10 this election that you can imagine, and more. 11 JOHN CATSIMATIDIS: How can that happen in 12 the United States of America? I mean, I -- I 13 don't understand what's going on with our Attorney General that just resigned, what -- what's going 14 15 on with the FBI that's supposed to be 16 investigating these things. I -- I mean, what say 17 you? 18 SIDNEY POWELL: We have a complete failure 19 of our institutions from the law enforcement 20 through the Department of Justice, to our courts 21 right now. 22 They're throwing out all the cases on, 23 quote, standing, end quote. Well, if congressmen 24 and electors don't have standing, and electors have standing under the constitution to bring a 25

```
1
     lawsuit challenging the election, who in the world
 2
     does?
 3
           It -- it's absolutely insane.
                                          There is
 4
     massive, massive, trillions and trillions of
 5
     dollars of global wealth behind this, what is
     really a coup of the United States of America.
 6
 7
     It's a blatant (phonetic) communist coup.
           JOHN CATSIMATIDIS: Who is more
 8
 9
     responsible, you think the -- the Chinese are more
10
     responsible or -- or is there any group of people
11
     more responsible than others?
12
                           The -- the Chinese are
           SIDNEY POWELL:
13
     largely responsible; Iran was working with them.
14
     We have attached to our exhibits at
15
     defendingtherepublic.org and kraken-wood.com, and
     SidneyPowell.com.
16
                        You can read the exhibits that
     we filed in court, that not a single judge has
17
18
     paid a bit of attention to.
           One might have said he did, but there's no
19
     way you can read the evidence and comprehend
20
21
     what's in there, and then dismiss it for failing
22
     to state a claim or standing, or any other reason.
     It's -- I've never filed a complaint with so much
23
24
     evidence behind it with the original filing.
25
     never seen --
```

```
1
           JOHN CATSIMATIDIS:
                               Roberts --
 2
                               -- a blatant evidence
           JOHN CATSIMATIDIS:
 3
     of fraud.
 4
           JOHN CATSIMATIDIS:
                               The -- the -- the
 5
     Justice Roberts, there's rumors that he was
 6
     yelling at the other justices; what have you heard
 7
     about that?
 8
                           I heard from a couple of
           SIDNEY POWELL:
 9
     sources that he was yelling at the other justices,
10
     and I don't know what's going on with Justice
11
     Roberts or the Supreme Court at all.
12
           I mean, these are the most important issues
13
     the republic has ever faced, and they're not even
14
     reconvening until the 8th of January.
15
           We have four cases pending there affecting
16
     Nevada with -- I'm sorry -- Wisconsin, Arizona,
17
     Michigan and Georgia; more than enough to change
18
     the results of the election, and they're just
19
     sitting on it.
20
           JOHN CATSIMATIDIS: And -- and it is
21
     mind-boggling.
22
           And Attorney General Barr, who just
23
     resigned, I heard that his brother -- I mean, they
24
     must have had something on Barr, my opinion,
25
     or our previous attorney -- I've heard that his
```

```
1
    brother hired Jeff Epstein at the location that
 2
     he -- his brother was at, it's a private school in
 3
     New York, and is it possible it's something like
 4
     that?
 5
           SIDNEY POWELL: I have no idea, John.
     I -- I am so disappointed I could -- if I were
 6
 7
     prone to tears, I would just sit down and cry.
 8
     really had --
 9
           JOHN CATSIMATIDIS: Well, you finally
10
     got justice -- you finally got justice with
11
     General Flynn, and that --
12
           SIDNEY POWELL: Yes.
13
           JOHN CATSIMATIDIS: -- Judge Sullivan
     signed off after Flynn was pardoned by the
14
15
     President.
16
           SIDNEY POWELL: Yes.
                                 That -- that whole
17
     scenario just amplified and -- and showed the
     world the corruption of our federal judiciary
18
19
     right now; whether it's just political corruption,
20
     financial corruption -- I don't know what it is,
21
    but it is -- it's the worst state of affairs this
22
     country has ever been in.
23
           JOHN CATSIMATIDIS: Georgia, the Senate
24
     race on Tuesday; what's going to happen, do we
25
     have enough checks and balances in place?
```

```
1
           SIDNEY POWELL:
                           I'm afraid we don't, John.
 2
     I mean, I'm encouraging everyone to get out and
 3
     vote, and break the algorithm again.
                                           But why
 4
     we're having a -- an election when we don't even
 5
     know that the two people in the runoff should be
     the two people in the runoff or that there should
 6
 7
     be a runoff at all, frankly, because the original
 8
     election was invalid.
                            That's something else I
 9
     don't understand.
10
           And -- and Lin Wood sued to stop the -- the
11
     runoff election and got poured out on that, too.
12
           JOHN CATSIMATIDIS:
                               It -- it's really --
13
           SIDNEY POWELL: -- (inaudible) --
14
           JOHN CATSIMATIDIS: -- mind-boggler --
15
           JOHN CATSIMATIDIS: -- courts -- yeah, it
16
          It's absolutely mind-boggling for any
17
     rational person to watch what's happening in this
18
     country right now. And anybody who is not
19
     demanding transparency in this election is part of
20
     the problem.
21
           There's absolutely no reason not to have a
22
     completely transparent election, unless you're
23
     pulling off a fraud. In fact, our federal laws --
           JOHN CATSIMATIDIS:
24
                               I told --
           JOHN CATSIMATIDIS: -- requires records to
25
```

1 be kept for 22 months under criminal penalty of --2 of a fine and one year in prison; and here we have 3 people destroying records right and left. adjudication file wasn't kept in Michigan for this 4 5 year; it was kept for prior elections, but not for this year. And that's because it would have 6 shown, no doubt, how Dominion people threw the -the ballot count from Trump to Biden. 8 9 JOHN CATSIMATIDIS: We have a minute left; 10 what would you tell the American people? 11 SIDNEY POWELL: We need to get loud and get 12 personal, and make our voices heard. I -- I am 13 encouraging people at this point, the state 14 legislatures are closest to the people, they have 15 full authority to uncertify or stay, or whatever, 16 their selection of electors, because they have certified fraudulent votes, is what they have 17 18 done, by choosing any slate of electors for Biden 19 whatsoever. That needs to be stopped right now. 20 21 shouldn't wait until January 6th. So pressure on 22 state legislators, make your voices heard; if you 23 have to stand with Trump signs and flags and 24 American flags around the outside of their houses, 25 do that. They need to know that the American

```
1
    people are awake, and know what happened in this
 2
     election, and will not tolerate a fraudulent
 3
     election.
           We cannot allow the United States of
 4
 5
     America to experience a coup by communists through
 6
     a fraudulent election or any other way, for that
 7
     matter.
 8
           JOHN CATSIMATIDIS: And what -- and the
 9
     communists are using the cash.
                                     There's an old
10
     expression in New York: Follow the money. And --
11
           SIDNEY POWELL: Exactly.
           JOHN CATSIMATIDIS: -- all the sudden all
12
13
     this cash has been floating around and -- and
14
     people have become rich over selling out our
15
     country.
16
           SIDNEY POWELL:
                           Exactly. And when money
17
     doesn't work, they use blackmail or threats.
                                                   They
18
     are evil.
                They intend to take all of our
19
     resources, like they've done in other countries
20
     around the world.
                        This must be stopped now.
21
           JOHN CATSIMATIDIS: Sidney Powell, thank
22
     you for being such a patriot and loving our
23
     country, and we're all behind you. We want -- we
24
     all believe one American, one vote and -- and
25
     whichever way -- if that can be verified, one a
```

```
(inaudible) -- on American, one vote, whichever it
 1
 2
     goes, I'll happy that way. But God bless America,
 3
     and God bless you.
 4
           SIDNEY POWELL:
                            Thank you, John. You, too.
 5
           JOHN CATSIMATIDIS:
                                This is the Cats
 6
     Roundtable. We'll be right back.
 7
           (End of the recording.)
 8
 9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
```

1	CERTIFICATE
2	
3	I, Jackie Mentecky, do hereby certify that
4	I was authorized to transcribe the foregoing recorded
5	proceeding, and that the transcript is a true and
6	accurate transcription of my shorthand notes to the best
7	of my ability taken while listening to the provided
8	recording.
9	
10	Dated this 3rd day of January, 2021.
11	$\Lambda = \Lambda$
12	Man V S
13	Grant to the
14	
15	
16	Jackie MENTECKY
17	
18	
19	
20	
21	
22	
23	
24	
25	

Exhibit 104

```
1
 2
 3
 4
 5
                                FILE NAME:
 6
              Tucker - More thoughts on Trump campaign
 7
                         Attorney Sidney Powell
 8
                               (1:38 min)
 9
10
11
12
                    TRANSCRIPT OF VIDEO RECORDING
13
                             TUCKER CARLSON
14
15
16
17
18
19
20
21
22
23
24
    Transcribed By:
    TERRI NESTORE
25
    CSR No. 5614, RPR, CRR
```

1

2

3

4

5

6

8

9

10

11

12

13

14

15

16

17

18

19

20

21

2.2

23

24

25

TUCKER CARLSON: Well, last night, in a segment about voter fraud and investigations into it, we told you about Sidney Powell, the former federal prosecutor, and her claim that roughly 7 million votes were secretly changed on election night by vote -- rigged vote counting software. Well, in the last 24 hours since we did that, we've heard from a lot of people about that segment, including people in the Whitehouse and people close to the president. Like us, they have concluded this election was not fair. Like us, they are willing to believe any explanation for what happened. Like us, they have not seen a single piece of evidence showing that software changed votes. It doesn't mean it didn't happen. It might have It means they haven't seen any evidence that it happened. And by "they," we are including other members happened. of Donald Trump's own legal team. They have not seen Powell's evidence either. No testimony from employees inside the software companies, no damming internal documents, no copies of the software itself. So that's where we are. Sidney Powell came on Fox this morning and suggested we may not have to wait much longer. I fully expect, she says, that we will be able to

```
1
    prove all of it in a court within the next two weeks.
 2
             Well, as far as we're concerned, that is great
 3
           If Sidney Powell can prove the technology companies
    switched millions of votes and stole a presidential
 4
 5
    election, she will have almost single-handedly uncovered
    the greatest crime in the history of this country, and
 6
 7
    no one will be more grateful for that than us.
 8
             (End of recording.)
 9
10
11
12
13
14
15
16
17
18
19
20
21
2.2
23
24
25
```

1	CERTIFICATE
2	
3	
4	I, TERRI NESTORE, Certified Shorthand Reporter/
5	Transcriptionist, do hereby certify that I was authorized
6	to transcribe the foregoing recorded proceeding, and that
7	the transcript is a true and accurate transcription of my
8	shorthand notes, to the best of my ability, taken while
9	listening to the provided recording.
10	
11	I further certify that I am not of counsel or
12	attorney for either or any of the parties to said
13	proceedings, nor in any way interested in the events of
14	this cause, and that I am not related to any of the
15	parties thereto.
16	
17	
18	Dated this 18th day of December, 2020.
19	
20	Talli Nastors
21	TERRI NESTORE, CSR 5614, RPR, CRR
22	TERRI NESTORE, CSR JULY, RER, CRR
23	
24	
25	

Exhibit 105

1	
2	
3	
4	FILE:
5	Fox's Maria Bartiromo Challenges Trump Lawyer Sidney
6	Powell to Provide Evidence of Wild Commie Conspiracy
7	Here's How That Went
8	
9	
LO	
L1	
L2	
L3	
L 4	
L5	
L6	
L7	
L8	
L9	
20	
21	
22	
23 24	
25	

1 MARIA BARTIROMO: Rudy Giuliani alleging 2 widespread election fraud at a press conference 3 yesterday. He said that the number of flawed ballots 4 5 is more than double the margin that Joe Biden won 6 in key states. The campaign alleging the following: 8 Number one, observers were prevented from viewing 9 mail-in ballots. 10 Number two, officials were told not to look for ballot defects. 11 Number three, they were told to backdate 12 13 mail-in ballots. 14 Number four, the Dominion Voting Systems 15 used in multiple states has ties to the Venezuelan 16 government, and votes were counted overseas. 17 Now, Dominion responded to Fox Business in 18 a statement. They say this: The latest flood of 19 absurdities is deeply concerning. Dominion is 20 plainly a nonpartisan American company with no 21 ties to Venezuela or Cuba. Vote counts are 2.2 conducted by county and state election officials, 23 not by Dominion, or any other election technology 24 company. That is from Dominion. 25

1 Joining me right now over the phone right 2 now to respond to all of this is the attorney for 3 President Trump, former federal prosecutor herself, and the author of the book Conviction 4 5 Machine, Sidney Powell. Sidney, thanks very much for being here. 6 7 want to first off -- start off with your response 8 to what Dominion says. Dominion is calling all of 9 the allegations that you and Rudy Giuliani and 10 Jenna Ellis have made absurd. Your response. 11 SIDNEY POWELL: It's almost laughable, 12 they've closed up their offices and moved 13 elsewhere. A hundred of their employees have 14 eradicated (inaudible) of their affiliation from -- with Dominion from their LinkedIn accounts. 15 16 They're fleeing like rats leaving the sinking 17 ship. 18 So I think there's a whole lot more there 19 than they care to discuss. They also declined to go to -- in front of the Pennsylvania legislature 20 21 today who wanted to ask questions of several of 2.2 their officials. 23 So they have a -- they have a very serious 24 problem. They created this system in Venezuela 25 for Hugo Chavez to rig the elections and make sure

```
They've sold that for that very purpose
 1
    he won.
     to other countries, and they brought it to this
 2
 3
     country for that very purpose. And they've used
 4
     it that way; we've got evidence that shows it.
 5
           We have firsthand testimony of witnesses
     who saw it happen, know how it was developed, know
 6
     why it was developed; and so it worked to achieve
 8
     its purposes. And many others. And we have
 9
     irrefutable statistical and mathematical evidence.
10
           MARIA BARTIROMO:
                             Sidney, what do you make
11
     of this --
12
           SIDNEY POWELL:
                          (Inaudible) --
13
           MARIA BARTIROMO: -- of this Eric Kumer,
14
     who -- who has been written about in -- in the
15
     press, he's the (inaudible) vice president of U.S.
16
     Engineering at Dominion Voting systems;
17
     apparently, he admitted on social media to rigging
     voting machines in order to prevent President
18
19
     Trump from winning re-election. He's an activist.
20
     He's been very active on social media.
21
     apparently, he said to someone who -- it was
2.2
     overheard: Don't worry about the election, Trump
23
     is not going to win. I made blank-blank sure of
24
     it.
25
           Who is Eric Kumer and what do you know
```

1 about this individual? Well, he holds several 2 MARIA BARTIROMO: 3 patents on some of the things they used in the 4 voting machine; so he knows exactly how it works. 5 He knows how to use it. And we have information about him being in other countries for rigged 6 7 elections there. 8 We have pictures of him in other countries 9 with -- helping people rig elections. So he's got a long history of -- of accomplishing the results 10 11 that they want accomplished, and I'm sure it's --12 it's for money. 13 MARIA BARTIROMO: All right. Sidney, I --14 I want you to respond to what Tucker Carlson said last night, Sidney. I don't know if you watched 15 16 it, but Tucker Carlson said that he invited you on his show to share evidence of -- (inaudible) or 17 18 flipping votes, and he -- he said you got angry and refused to provide evidence for your claims of 19 20 voting software flipping votes. 21 How do you respond Tucker Carlson, did you 22 get angry with the show because they texted you 23 and asked you to please provide evidence of what 24 you're alleging? 25 No, I didn't get angry MARIA BARTIROMO:

1 with the request to provide evidence. In fact, I 2 sent an affidavit to Tucker that I had not even 3 attached to a pleading yet to help him understand the situation. And I offered him another witness 4 5 who could explain the mathematics and statistical evidence far better than I can. I'm not really a 6 7 numbers person. But he was very insulting, 8 demanding and rude, and I told him not to contact 9 many again in those terms. 10 So -- so, Sidney, will MARIA BARTIROMO: 11 you be able to prove this evidence that you say you have of this technology flipping votes from 12 13 Trump to Biden, how will you prove that, Sidney? 14 MARIA BARTIROMO: Well, we have witnesses 15 that know how it's done and they've seen it done, 16 Maria. That's firsthand evidence of -- of how it 17 works, and -- and that it works. 18 And we'll -- we will also have a lot more 19 evidence as the days progress. I mean, I'm still 20 getting information through a (inaudible). 21 can't even keep up with the witnesses that are 22 calling in and wanting to give affidavits and 23 provide evidence. 24 So this was very early in a stage of any 25 case, aside from one of this massive magnitude

1 that, frankly, should have been investigated and 2 stopped by our law enforcement community within a 3 -- a decade ago. So we shouldn't be in this 4 position, and here we are, a few -- a handful of 5 -- of civil lawyers trying to do the work of a massive government institution in the biggest 6 7 worldwide corruption fraud ever exposed. So -- so Sidney, what 8 MARIA BARTIROMO: 9 about this comment from the Dominion side saying: 10 We have no ties to Venezuela. 11 What specifically are the ties to 12 Venezuela? You and Rudy said that our votes in 13 America go back to a foreign land, that they -they are looked at and processed, potentially, in 14 15 Europe. Dominion is saying we have no ties to 16 17 Venezuela, no ties to Cuba. Can you explain that? 18 SIDNEY POWELL: All I can tell you is that 19 -- well, the company might have somehow severed or tried to sever the relationships recently. 20 21 don't know how they are parsing their words. 22 I can tell you that the company was started with 23 Venezuelan money, in Venezuela, for the express 24 purpose of rigging elections for Hugo Chavez. 25 We have people that were there at his side

1 while it was all done. They were in the control 2 room and watched how the votes were flipped. 3 can -- to -- can watch the votes in realtime. We 4 have evidence now of information from the systems 5 going to three or four different foreign countries during the time of the election so they -- those 6 countries themselves could have watched the live votes come in and changed the numbers. 8 9 There's significant evidence of foreign interference from the -- of the worst communist 10 countries on the earth with our election. 11 Now, Sidney, Rudy 12 MARIA BARTIROMO: 13 Giuliani last night was on Hannity, and he said 14 this had to come from someplace in the Biden 15 campaign, as an instruction to all of them, 16 because he said that once you had a flaw in one 17 Dominion machine, you saw a similar flaw in many 18 different machines. 19 So what was Rudy referring to, that this 20 had to come from someplace in the Biden campaign 21 as an instruction to all of them, Sidney? 22 SIDNEY POWELL: I don't know what specific 23 evidence he was referring to. We've had to divide 24 and -- and -- to conquer this monster that we're 25 facing; and I am focusing more on the technology

1 and the fraud, and he is working the individual 2 witnesses on -- on that side of things. 3 haven't even --4 MARIA BARTIROMO: Okay. 5 SIDNEY POWELL: -- had time to --6 MARIA BARTIROMO: Sidney, let me ask you 7 this: A -- a lot of people out there want to 8 believe what's happening and what you are 9 presenting, because they want to make sure that 10 this was a fair election, and they want to make 11 sure that their vote counted. 12 Do you believe that you will be able to 13 prove this in court in the next two weeks? 14 recognize you -- you have said, and Jenna Ellis 15 We're not litigating this for the has said: 16 public media, we're not on a TV show; we want the 17 courts to see the evidence, and it may go up to 18 the Supreme Court. 19 You've got about two weeks, Sidney; will 20 you be able to present, are you planning to 21 present, actual evidence of all that you've said, 22 Dominion voting machines, swapping votes from 23 Trump to Biden, as well as an effort to actually 24 change the results of an election, you'll be able 25 to prove that in court in the next two weeks?

1 SIDNEY POWELL: Yes, I fully expect we will 2 be able to prove all of it in court within the 3 next two weeks; although, the fraud case itself doesn't have to be done within the two weeks. 4 5 we have more than enough evidence now -- we have more evidence now than half the prison population 6 is imprisoned on, of this egregious fraud. 8 I mean, the evidence --9 MARIA BARTIROMO: The other thing I wanted 10 11 SIDNEY POWELL: -- is really stunning, 12 Maria. 13 MARIA BARTIROMO: Really? Okay. What's --14 what's the most stunning, the most egregious? 15 Give me one thing that's the most egregious and 16 most stunning, Sid- -- Sidney, as -- as we wrap up 17 here. 18 SIDNEY POWELL: Well, one of the most 19 impressive pieces of evidence is the affidavit of 20 the young military officer who saw it all done and 21 was there when it was created. He knows exactly 2.2 how it works. He was briefed on it. And many 23 other people are talking every day about how it 24 worked. 25 We've got Eric Kumer, as you said,

1 admitting on -- on tape that he rigged the 2 election for Biden and hated Trump. 3 their social media posts. We've got all kinds of 4 evidence that -- that is mathematically 5 irrefutable by experts; including three professors at Princeton, and it all wraps up and proves the 6 7 same thing. 8 The en- -- the -- the evidence of 9 individual poll watchers who saw votes come in, 10 saw the machines manipulated; the machines are 11 never supposed to be hooked up to the Internet, at 12 least 30 of them were, according to a published 13 article that's already out. 14 That's an egregious breach of election law 15 in itself. That should never have happened. 16 causes automatically -- that should automatically 17 invalidate anything coming out of those machines 18 in every state that happened in, if not across the 19 country, because they can change everything as 20 they're watching it. 21 Okay. All right. MARIA BARTIROMO: 22 Sidney, thanks very much. We, of course, will be 23 on this and keep following it. 24 Sidney Powell, thanks for joining us. 25 with us at the (inaudible). We'll talk once again

```
1
     with the attorney for President Trump Jenna Ellis.
 2
            (End of the recording.)
 3
 4
 5
 6
 8
 9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
```

1	CERTIFICATE
2	
3	I, JACKIE MENTECKY, do hereby certify that
4	I was authorized to transcribe the foregoing recorded
5	proceeding, and that the transcript is a true and
6	accurate transcription of my shorthand notes to the best
7	of my ability taken while listening to the provided
8	recording.
9	
10	Dated this 31st day of December, 2020.
11	$\Lambda = \Omega_{\alpha} I_{\alpha} = \Lambda$
12	1 March V X
13	Charles to the
14	
15	<i>'</i>
16	JACKIE MENTECKY
17	
18	
19	
20	
21	
22	
23	
24	
25	

Exhibit 106

screenshot-twitter.com-2021.01.06-13_57_32 https://twitter.com/realdonaldtrump/status/1327811527123103746 06.01.2021



I look forward to Mayor Giuliani spearheading the legal effort to defend OUR RIGHT to FREE and FAIR ELECTIONS! Rudy Giuliani, Joseph diGenova, Victoria Toensing, Sidney Powell, and Jenna Ellis, a truly great team, added to our other wonderful lawyers and representatives!

10:11 PM Nov 14, 2020 - Twitter for iPhone

66.1K Retweets 9.8K Quote Tweets 325K Likes

Exhibit 107

Case 1:21-cv-00040 Document 1-106 Filed 01/08/21 Page 2 of 31 Global Prayer U.S. Election Integrity

```
1
 2
 3
                          File:
 4
     Global Prayer for U.S. Election Integrity
 5
 6
 7
 8
 9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
```

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

2.2

23

24

25

SPEAKER: At -- this time we are so honored to have with us at -- at a very critical juncture Sidney Powell; just a renowned a -- attorney. She represented Michael Flynn, who was with us a couple weeks back, and she's representing a lot of cases on this election integrity, exposing the election fraud, so that we can re-establish President Trump as the legitimate winner of the elections, and our next President for four years. Sidney, thank you so much for joining us. Are you able to speak from where you're at? Thank you for having me on. SIDNEY POWELL: Thank you for your prayers and support. We've -our team -- whole team feels it. We have had information come at us from multiple different directions. I -- I can see God's hand in sending us things we need when we need it. And it's been a -- a huge honor to work on this project. We must get to the truth of this election, the American people are entitled to and are starved for the truth. The bottom line question I always ask is: Why is it so hard to look into the machines? There shouldn't even be an issue about that. Federal law requires people to keep all election

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

2.2

23

24

25

information for 22 months, under penalty of -- of criminal prosecution with up to a year in prison and a fine. Well, that's because our elections are supposed to be transparent. This is one country in the world where we're supposed to be able to count on one person, one vote. And what we've gotten this year, we've finally seen it in real-time, is an algorithm being run to shave a substantial portion of the votes so that Mr. Biden got 1.26 in many places, and a Trump vote was weighed at .74. That's absolutely outrageous. It's supposed to be one person, one vote. should be no fractions of any votes calculated anywhere. But we're getting more and more information that the algorithm ran in lots of places, including in the red states and against red counties. And that's probably what they ran in 2016 that left Hillary Clinton with the popular vote total being higher than Trump's. That's the only thing that explains that, frankly. And it explains a lot of other things, too.

And then there are particular places where so many Trump people poured out to vote on

1 election day, which is what we all encouraged them 2 to do, to wait for election day and vote in person 3 to make sure their vote got counted, that they 4 broke the algorithm in all the swing states that 5 they had pre-calculated, based on the pre-election voting. And -- and that's why the voting had to 6 7 count -- stopped counting in multiple states that night when we saw it all happen. 8 And then 9 suddenly, you know, Biden votes appear. 10 We've now traced some of the injected fake 11 ballots to a mail facility in New York that isn't even authorized to take mail, it takes freight. 12 13 And -- and there's a -- several hundred-thousands 14 of ballots we have information and evidence now 15 was put through that mail facility, and that's how 16 it was injected into the system to then get to 17 different states, like Pennsylvania where all of a sudden hundreds of thousands of votes manifested 18 19 themselves after counting had supposedly stopped. 20 SPEAKER: Sidney? 21 SIDNEY POWELL: Yes. 2.2 SPEAKER: Yeah. Can you hear us? 23 SIDNEY POWELL: Did I lose you? 24 SPEAKER: Yeah. No, you're fine. Go 25 ahead.

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

2.2

23

24

25

SIDNEY POWELL: Okay. So -- SO we've seen every manner and means of fraud that anybody can imagine, but it's the machine fraud that I think is the absolute most insidious; that coupled with the fake ballots that they used to backfill the vote count the night of the election that were shipped through our United States mail service; which is, by the way, a federal mail fraud crime, because we know that hundreds of thousands of ballots were sent that way, and they weren't shranked. (Phonetic). So that's -- that's a massive mail fraud offense in more ways than one. SPEAKER: Okay. SIDNEY POWELL: And, of course, we're getting more evidence now, too, on the paper Jovan Pulitzer is in Atlanta now, we've issues. got more information coming out about the internet connections that the Dominion machines had. know that information was uploaded to them by thumb drive; that was impermissible. There should have been nothing changed on the machines from several days -- maybe even 30 days, I can't remember the exact number before the election,

until after the votes were tallied and everything

properly counted and accounted for.

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

2.2

23

24

25

On the machine we got access to in Antrim County, Michigan -- or the machines, I should say -- they found a substantial flip rate of the votes. And even worse than that, the machines were calibrated to send the vast majority of votes into what's called an adjudication file that Dominion has on their machines, that then allows an individual to decide where those votes go. Well, we're talking about hundreds of thousands of votes going in an adjudication file, I think in Fulton County, Georgia, they found that over 92 percent of the votes went into an adjudication file. That's hundreds of thousands of votes that were then all of a sudden -- any number of them disappeared for Trump or reappeared as if they were Biden votes to a substantial percentage. In fact, one number at one point was 186,000 votes all for Biden, with -- those are mathematical and statistical impossibilities. It's like flipping a coin the same time, and it's 186,000 times and it lands on heads every time. It does not happen. So there are all kinds of charts and mathematicians and statisticians who have looked at these things from every different angle, and

1 there's no way that Donald Trump lost this 2 election by any legitimate means. multiple means of fraud, but the two biggest are 3 the false ballots that were fed into the machines 4 5 after they stopped counting on election night in all the swing states -- and probably other states, 6 too -- and then the embedded machine fraud -- and 8 that's why we want to audit the machines. 9 Everyone who cares about fairness and 10 integrity in this election or wants us to ever have another free and fair election, this must 11 12 stop right now. It cannot continue past this 13 election or there will never be another free 14 election. 15 Sidney, we have a couple SPEAKER: 16 We -- we understand how rampant the questions. 17 fraud is, but time does not seem to be on our 18 side. 19 Can you describe the January 6th joint session of Congress constitutionally, if these 11 20 21 to maybe a few more senators go in on their 22 petition requesting a stay of -- of certifying the 23 elect- -- Electoral College on January 6th, and 24 asked for 10 days to set up a council to review 25 the fraud, could you go over the -- the

1 constitutionality of that, what the Vice President 2 can do, does he have an authority presiding to 3 stay the -- the voting at that time? 4 SIDNEY POWELL: Yes, I think either he or 5 the President, frankly, could stay the vote. I think it should be mandatory that an independent 6 7 forensic audit be conducted of a number of the Dominion voting machines. And, frankly, other 8 9 voting systems. It's not exclusive to Dominion. 10 The DNA of the -- of the code that can run the 11 algorithms and -- and accomplish the cheating 12 exists in all the systems. 13 So we don't know exactly how widespread it 14 I think there should be a random sampling of 15 at least a dozen different locations in big cities 16 to check what's going on with the machines. For example, in Antrim County, we know that 17 18 somebody destroyed the adjudication file audit trail for the Dominion machines there. 19 That -that's a violation of federal law in and of 20 21 itself. Somebody should be prosecuted for that 2.2 right now. 23 And while I'm on the subject of 24 prosecution, just let me say how appalled I am at 25 our Department of Justice and FBI for not being

all over this. They are obviously part of the problem. I have maintained for a long time that this software probably initiated with the CIA, and our own government is implicated in a lot of the wrongdoing here; and that's why the cover-up is so massive, and there's so much resistance, aside from the trillions of dollars of global wealth and all the corrupt dictators that have been installed around the world, people thinking they're actually voting for the person they want, and instead their vote is rigged by this kind of system.

As far as your cases, do -- do you have anything that's set to go before the Supreme Court in the next couple of days, we saw that Justice Roberts -- I think it was one of your cases, would not hear it until I think after the certification or after Inauguration Day; is there --

SIDNEY POWELL: Right. That's another point of -- of being disgusted with our current system. We -- we're really seeing institutional failure at every level of our government. It's -- it's terrifying, frankly, to have the republic of the United States of America, the last great country in the free world, in this sort of position with the complete institutional failure.

2.2

But the Supreme Court isn't even going to meet again until the 8th, and we have four cases pending there involving the states of Arizona, Michigan, Wisconsin and Georgia. Any three of which, if I recall correctly, are sufficient to flip the election.

There are also a couple of Pennsylvania cases pending, fraud was rampant in Pennsylvania. In fact, we know that several hundred thousand ballots were trucked there to backfill the night of the election. And, of course, we've seen bins of them being unloaded from underneath the table in Fulton County, Georgia on video.

So anybody that's saying there's no evidence is not looking at the evidence, and is either willfully blind, corrupted by the Chinese communist party, blackmailed by the Chinese communist party, or has some kind of skeleton in their closet that somebody else is holding over them. There's no other logical rational excuse for any intelligent person not to see the blatant fraud here. They took the two worst candidates in the history of the republic, probably, and crammed them up our nose with fraud, so blatant that multiple mathematicians the night of the election

1 saw it happening from all over the country. 2 If we can just walk through that 3 plan that Ted Cruz is leading with the 11 or 12 4 Senator -- assuming the Vice President or the 5 President agrees to stay the count on January 6th It's a -- not a mandatory 6 for 10 days. 7 commission, a commission is established, they come 8 back and then what? They present it and there has 9 to be a -- a vote be- -- in the House and the 10 Senate to override, where does it go from there? SIDNEY POWELL: Well, I have had my head 11 12 down working myself, and I can't say that I'm 13 completely familiar with Senator Cruz's plan. 14 Personally, I'm not in favor of some sort of 15 political commission that goes in to look at that. 16 We need computer and cyber experts. There is 17 evidence out there already that there was foreign interference in this election, and until credible 18 19 professional law enforcement, cyber security experts, military experts, a combination of the 20 21 above, look at what happened in the Dominion 22 machines and certifies that under penalty of 23 perjury and produces the audit trails and all the 24 paper and everything else, no one should be satisfied with the -- the fraudulent result of the 25

```
1
     -- of the, quote, Biden election, end quote.
 2
           If there's nothing to hide, they should be
 3
     hiding nothing.
 4
                     Jim, you have a question?
           SPEAKER:
 5
           JIM:
                 Yeah, I -- I do, Sidney.
                                            Thank you
     for coming on with us, and thank you for paying
 6
 7
                None of us can probably imagine the
     the price.
 8
     price you are paying for standing for truth, as
 9
     you are.
10
           When Mario alluded to we're running out of
     time, that's an understatement; we are out of
11
     time, we're three days away from a major event in
12
13
     D.C.; as we know, 17 days away from a scheduled
14
     inauguration. Some of what you're describing that
15
     needs to happen sounds like it would be court
16
     cases and forensic work, it would be over the next
     two years to solve. We don't have that, at least
17
18
     not right now.
19
           So what are our options -- what -- in all
     the times that you or anybody else for this issue
20
21
     has taken something to court, has -- as -- has
2.2
     there ever been a court that has listened or they
23
     rejected every case that's come before us, have we
24
     had any wins in court so far?
25
           SIDNEY POWELL: No, they're throwing them
```

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

2.2

23

24

25

all out on the DNC talking points of no standing, no matter who you are; or they're just sitting there like they are at the Supreme Court now, where we know our cases have standing because we represent electors in my four cases, who have standing under the constitution. They're named in the constitution. They clearly have standing. But the District Court poured us out on that in Georgia, and so did the courts in the other three states, because that's the litany the -- the democratic machine or the establishment machine -- whatever you call it -- are pushing here. And -- and like I said, the corruption is far wider and deeper than any one of us would have ever imagined. It's really shocking to not have Article 3 judges who are given lifetime tenure for this very reason, stand up for the rule of law and the future of our republic. They say: Oh, it's political, so they really don't want to get involved in it. they make up these legalistic excuses for not doing their jobs. None of which is acceptable. But we know people have been threatened, our

witnesses have been threatened, people have been

```
1
     intimidated right and left. I wouldn't be
 2
     surprised if that hadn't happened to some judges,
 3
     too.
 4
           SPEAKER:
                     So there's not been a single
 5
     judge who has listened to a single case; is that a
 6
     true statement?
           SIDNEY POWELL: No, that's true.
                                              No iudae
     has actually listened to the evidence.
 8
                                              And the
 9
     few that have ruled on anything have done it so
10
     fast on purely legalistic grounds, not looking at
11
     the evidence, that even if they say: Oh, yeah; I
12
     looked at the evidence -- well, we're talking 270
13
     pages of affidavits, 530 pages of affidavits.
14
           And by the way, all the affidavits and
15
     evidence -- at least of the time of our Supreme
16
     Court filing are uploaded and available for people
     to look at and download free on the website
17
18
     defendingtherepublic.org or kraken-wood.com or
19
     Sidneypowell.com.
           Read the evidence for yourself. There are
20
21
     videos online that show the Dominion activities
2.2
     and other activities that are clearly illegal.
23
     It's -- it's everywhere. It's available on
24
     Twitter. Educate yourself. Look for yourself,
     judge for yourself.
25
```

1 JTM: Sidney, to what extent is there a 2 healthy system of coordination between a Senator -- such as Senator Cruz, for example -- or Holly 3 4 from Missouri, and state senators -- I -- I just 5 came off a call where I -- where I saw what it seems to me to be a lack of communication 6 7 coordination and -- and --8 SIDNEY POWELL: That also --JIM: -- other persons -- other persons 10 like yourself, how connected are you all so you're 11 moving as a common force together as one? SIDNEY POWELL: Well, I think you all are 12 13 doing a lot to facilitate that -- that common 14 goal. I mean, it's been such a short amount of 15 time and we've been dealing with such a flood of 16 information, nothing has been as coordinated as it certainly should have been and would have been 17 more effective if it had been. 18 19 In fact, there have been unnecessary factions, from my perspective, of what to focus on 20 21 and how to focus on it. But we're -- where we are 2.2 now -- and I would encourage all of you to start 23 with your -- bombarding your state legislators 24 tonight, because they are the closest to the 25 people, and they should be the ones to decertify

9

1 or decide to stay their electoral slates tomorrow 2 so it doesn't even get to Congress on the 6th. 3 SPEAKER: Yeah, I think Rob is going to go 4 over that. If you can -- everyone can put your 5 Zoom on -- on mute. Lance, do you have a question for Sidney -- Sidney? 6 Yeah. Well, I think these -- I'm just curious, and it might not be something, 8 9 Sidney, that you can address, but the mystery to 10 many of us who are kind of newly engaged with --11 with the -- the whole civic process, I think the 12 whole country is getting an education -- I 13 understand --14 SIDNEY POWELL: Yeah, a painful one. 15 It's a painful one, yeah. And I'm 16 mystified at the legislators in the state level 17 that are Republican that are not moving more 18 aggressively, because you would think that they 19 would have an interest in getting reelected, then I realized that our voices and -- we, as a people, 20 21 have not actually been communicating with them; 22 we've just been trusting that the civic process of 23 election -- what's going to work. 24 So now they're suddenly getting bombarded 25 and they're having an awakening like, oh, my gosh,

1 how many people are -- exist out there that are --2 that are upset about this? 3 But why do you think there's only 11 Senators standing with Ted Cruz, why is Josh --4 5 why is it that there aren't more Senators that are actually engaged with this, is -- do you have a --6 7 a thought on that, is that the power of money and 8 -- and --9 SIDNEY POWELL: It -- it is the -- yeah, it's the power of money, it's the power of 10 11 lobbyists. It's the fact that we don't know 12 exactly how long this has been going on. 13 know how many of our Republican officials have 14 been elected by virtue of machine fraud from any 15 of these voting machine companies. 16 We know that in 2019 Elizabeth Warren and Amy Klobuchar and four others signed letters 17 18 expressing serious concerns about the 19 vulnerability and problems with the machines. 20 We know that Carolyn Maloney was 21 complaining about it in New York back in 2013. 2.2 Apparently the problem has existed far 23 longer than I knew about it. But, again, I wasn't 24 political and wasn't paying attention, like a lot 25 of us are out there trying to support our kids and

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

2.2

23

24

25

do our jobs and do everything else we're supposed to do, and pay our taxes, while these people are ripping us off and taking boondoggles to communist China and wind up getting blackmailed as a result of the trip. You know, we don't know how many are in the pocket of communist China. We know Dianne Feinstein had a communist (inaudible) spy for 20 years. We know Eric Swalwell was sleeping with a communist spy. We have no idea how many have infiltrated our universities and politics and everything else, but it's a lot. They're stealing our technology right and left. This is a foreign interference in our election from communist China and Iran, and nobody wants to admit it, because it shows how vulnerable we are, how vulnerable we have been, how many government agencies have failed to do their jobs for at least a decade. This isn't the first year this happened. Was the Dominion --SPEAKER: SIDNEY POWELL: It's worst. SPEAKER: Was the Dominion software involved -- I thought I just heard you say once that -- that 130 votes were processed by that

1 software when Obama was elected; is that -- was 2 this software being used back then? SIDNEY POWELL: 3 I'm sorry. You're breaking 4 But yes, I'm sure the software was used in up. 5 2018, and somebody's given me a massive amount of data we haven't had time to deal with yet, that it 6 was used in 2016 when Hillary won California over 8 Bernie. 9 My witness told me that Bernie was told 10 about it and instead of outing it, he sold out. 11 SPEAKER: Okay. 12 Sidney, we were talking about 13 coordination, we know that you met with the 14 President -- I guess about two weeks ago, had --15 had a good meeting or meetings with him, and then 16 we read the press where you were not allowed to 17 speak to him -- et cetera, et cetera. Have you 18 been in touch directly or indirectly, if you can 19 -- if you can share -- with the President as far 20 as potential coordination? 21 SIDNEY POWELL: I have not been in touch 2.2 I had a very brief conversation about that. 23 later, he is aware of the fact that people have 24 kept me out. I don't know the reason for that. SPEAKER: Jim? 25 Okay.

```
1
           JTM:
                 When you were -- or -- the language
 2
     you were using a moment ago was focused on the
 3
     future elections, obviously based off what has
 4
     happened in 2020, I -- I had a bizarre question,
 5
     and that is: If you're successful -- and we pray
     you are -- in proving the illegalities of the 2020
 6
 7
     election, and maybe others as well, but
 8
     particularly the 2020 presidential election, what
 9
     is -- is there anything provided in our
10
     Constitution that would address retroactively a
11
     President who might have already been installed on
     January 20th of 2021, if it's later --
12
13
           SIDNEY POWELL: No, that's -- that's --
     yeah, that's what concerns me. We have to be able
14
15
     to fix this now, and the inauguration can be
16
     postponed if necessary. But the fraud -- the
17
     fraud cannot -- the fraud cannot be allowed to
18
     stand now.
19
           SPEAKER: A -- an inauguration can be
20
     legally postponed?
21
           SIDNEY POWELL: Yes, the inauguration can
2.2
                    It's happened at least once before
     be postponed.
23
     in -- in our history maybe more than once.
24
           SPEAKER: Does the current (inaudible) --
25
                           But yes, it's a -- it's a
           SIDNEY POWELL:
```

1 national emergency, frankly. The foreign 2 interference in the election that we know is 3 documented already by the FBI and the CISA, 4 triggers the President's powers under the election infrastructure and other election insecurities --5 or whatever the last Executive Order 13848 was on 6 the election interference, and that allows him to 8 do anything he needs to do. It triggers all his 9 national emergency powers. 10 So, yes, the election inauguration and 11 everything could be postponed. And the current President remains 12 SPEAKER: 13 as President past January 20th? 14 SIDNEY POWELL: Yes. 15 SPEAKER: Okav. 16 Even though it appears that DOJ SPEAKER: 17 and FBI have gone dark, do you know -- is there 18 any hope that they are doing something and we'll 19 hear something soon, as far as the foreign 20 interference with our Deep State? 21 Well, if the report I read SIDNEY POWELL: 2.2 was correct about Senator Cruz's meeting at the 23 White House that prompted his change of heart, he 24 was briefed by DOJ and by some in the intelligence 25 community, apparently, about the foreign

1 interference; and DOJ is starting to do something 2 about it. But there was a lot of domestic 3 4 interference, as well as foreign interference. 5 People no doubt acting as foreign agents here domestically. It's -- it's a big widespread 6 7 problem, and it has to be addressed now. 8 cannot sweep it under the rug again. 9 SPEAKER: Okay. And that's where if we can 10 get 10 -- a 10-day stay on the electorate 11 determination on January 6th, it could help; at 12 least expose that to the public and to the 13 Congress, if we had a few --SIDNEY POWELL: Exactly. And that 10 days, 14 15 frankly, is enough to do a substantial forensic audit in multiple states, on multiple machines. 16 17 We had a plan to do a -- a -- a fair sampling of 18 them in less than 10 days several weeks ago. And 19 that same plan could be triggered now, I just don't know why -- keep -- people keep stalling on 20 21 it, other than there's massive pressure to ignore 22 all of this and just -- you know, quote, move on, 23 end quote, and never have a free country again. 24 SPEAKER: Jim -- Jim has another question 25 just for all the listeners that are here in this

1 prayer meeting. I mean, one of the things 2 specifically -- and you can tell us what else to 3 -- to pray against the massive pressure that the -- the Lord can move and -- and encounter that 4 5 pressure against those that are exerting the pressure, which is intimidation and control, to 6 7 try to silence the truth to come out. 8 Jim? 9 :MTT Sidney, if you could give us in 10 layman's terminology the chief talking points, 11 you've said quite a bit tonight, but if you were 12 to -- if you were to be able to arm -- there --13 there's seven -- almost 8,000 of us on this call 14 right now, 8,000 screens, it could be many more 15 people than that, and many more will watch later, 16 if you were to give us three or four talking 17 points that a layman can understand and could articulate to other people, what would those be? 18 Well, I would start with 19 SIDNEY POWELL: the fact that it was a mathematical impossibility 20 21 for the things we saw happen on election night to 22 Any person with math expertise or 23 statistical expertise can see that people 24 identified it from various places across the 25 country -- in fact, around the world. I would

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

2.2

23

24

25

encourage everybody to look -- never in my lifetime have so many people come forward at great personal risk, loss of their jobs, being harassed, being threatened. A worker in Alabama -- or Georgia just had five shots fired through the window of her home last night working with Jovan Pulitzer on the ballot issues in Georgia right now. People have taken -- patriots have come forward all across this country to stake a -- take a stand against this massive fraud. And the bottom line is, if there's nothing to hide, why are they fighting so hard to hide it? This is the one country on earth where any election is supposed to be completely transparent, where all the records are required to be kept by federal law. There should be no question about it whatsoever. And any independent person should be able to go and see and count whatever needs to be counted, whether it's on a machine or whether it's paper; but running the same fraudulent ballots back through the same fraudulent machines is not a valid recount. And the fact that they are trying to avoid

```
1
     having any of the machines examined forensically
 2
     in any other place in Antrim County, Michigan,
 3
     tells me all I need to know to know that they are
     hiding massive evidence of fraud that goes a lot
 4
 5
     farther back and wider than this election, and
     that there's no telling how many people have
 6
 7
     benefited from it here and around the world,
 8
     including some Republicans.
 9
           SPEAKER:
                     Your first talking point --
10
           SIDNEY POWELL:
                           So what we need to pray for
11
     is the truth.
                    We need to pray --
12
                     Your first talking point --
           SPEAKER:
13
           SIDNEY POWELL: -- that the truth comes
14
     out, whatever that is, and the chips fall where
15
     they have to fall.
16
                     Sidney, can you continue with --
           SPEAKER:
17
     that's very persuasive, the mathematical
18
     impossibilities; and the second one I wrote is why
19
     would you hide it, why wouldn't it be in
     everybody's interest to know what the truth is.
20
21
           Any other key talking points you can give
2.2
     to us? Because there's quite a people -- quite a
23
     few people writing down what you're saying to use
24
     as talking points, Facebook and other -- other
25
     conversations.
```

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

2.2

23

24

25

SIDNEY POWELL: Yes. All the thousands of witnesses who have come forward at great personal risk to give their personal testimony of the fraud they've seen, and the video evidence of fraud happening in front of our eyes. Plus hundreds of thousands of -- of, quote, mailed ballots being brought into the system fraudulently through a freight facility in New York. That doesn't happen when they're real ballots. Thank you so much. SPEAKER: Uh-huh. SIDNEY POWELL: And -- and Dominion shredding everything -- I mean, Dominion has been shredding things right and left. Within a week of the election they shredded thousands of pounds of They moved their offices just across town in Denver -- and I believe elsewhere. shredding truck pulled up -- I don't even know how many thousand pounds were shredded within that first week. And -- and on top of that, they're shredding, literally as we speak in Georgia, they started it again the night Jovan Pulitzer testified in front of the Georgia Senate Committee, I think it was, and showed how the machines could be hacked in real-time in the

1 runoff election in Georgia. 2 Sid- -- Sidney, we want to thank 3 you so, so much for your time, for all that you've 4 been doing. I know you're -- you're very, very 5 busy. We just want to take one more minute to pray for you, for your legal team, for the -- for 6 7 the Lord to be with you. 8 Pam, can you please pray for Sidney. 9 Sure. Lord God, we thank you for PAM: 10 Sidney Powell and her entire team as they have 11 tirelessly fought for truth to come out. And God, 12 we pray for her that you would surround her with 13 warring angels. And God, we plead the blood of 14 Jesus over her. And we ask you to minister to her, Lord, and through her. 15 16 God, we pray that in these next few days, 17 Lord, that there would be such a turning. 18 Lord, you would give her strategies from heaven. 19 This is a -- a spiritual battle with angels and 20 demons warring over America. And God, we cry out 21 tonight on this prayer call for strategies from 22 heaven to be given to her, the legal team, for our 23 President and his team, Lord God, that you will 24 move mightily. 25 And we thank you, Lord. Lord, I -- I can't

1 even imagine the amount of warfare that is -- is 2 coming against her, Lord, as she is fighting for 3 righteousness and truth, and for the American 4 people. 5 And God, I ask you to give her strength, 6 both physically. And God, just legally, Lord, 7 that you give her such strategies. And we thank 8 you, God. And we thank you ahead of time, Lord, 9 for victory. And Lord, that we are going to see a 10 turning because, God, there are multitudes around 11 our country and around the world, standing in the 12 gap, crying out for truth. 13 Lord, keep your hand upon Sidney and her 14 team, and continue to use them. And I thank you 15 for her, Lord. And I thank you for her team. 16 And Lord, we do declare victory. And we 17 thank you in Jesus name. Amen. 18 SPEAKER: Thank you so much, Sidney. Amen. 19 SIDNEY POWELL: Thank you so much. Thank 20 you very much. 21 We'll continue to be praying for SPEAKER: 22 you and being in touch with you. Thank you so 23 much. 24 SIDNEY POWELL: Thank you. And pray for our President and Vice President, and for the 25

```
1
     country as a whole. It's imperative we remain the
 2
     beacon of freedom for the entire world.
 3
                                        Thank you so
           SPEAKER: Amen. We will.
 4
     much.
 5
           SIDNEY POWELL:
                            Thank you. Bye-bye.
 6
           (Advertisement.)
 7
           (End of the recording.)
 8
 9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
```

1	CERTIFICATE
2	
3	I, Jackie Mentecky, Transcriptionist/Court
4	Reporter, do hereby certify that I was authorized to
5	transcribe the foregoing recorded proceeding, and that
6	the transcript is a true and accurate transcription of my
7	shorthand notes to the best of my ability taken while
8	listening to the provided recording.
9	
10	Dated this 4th day of January, 2020.
11	$\Lambda = \Lambda$
12	/ manufactor &
13	Charles to the state of the sta
14	
15	
16	Jackie Mentecky
17	
18	
19	
20	
21	
22	
23	
24	
25	

IN THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF COLUMBIA

US DOMINION, INC.,	
DOMINION VOTING SYSTEMS, INC., and))
DOMINION VOTING SYSTEMS)
CORPORATION,	
Plaintiffs,)
V.)
SIDNEY POWELL,) Case No
SIDNEY POWELL, P.C., and)
DEFENDING THE REPUBLIC, INC.,)
Defendants.))

NOTICE OF FILING EXHIBITS

1. Plaintiffs hereby give notice of filing exhibits listed below, which were exhibits to the Complaint filed on January 8, 2021 [D.E. 1]. Due to their nature, they are unable to be filed electronically through the Court's ECF System. Therefore, a transcribed copy of each exhibit has been electronically filed through the Court's ECF System with the corresponding Exhibit Number.

Exhibit Number	Description	Location
5-V	Sidney Powell talks about her allegations regarding the computerized voting systems on election night, Washington Examiner (Nov. 20, 2020), available at, https://www.washingtonexaminer.com/videos/sidney-powell-talks-about-her-allegations-regarding-the-computerized-voting-systems-on-election-night (last visited Jan. 4, 2021).	This exhibit is maintained by counsel and is available upon request. As it is an audio/video, the exhibit is not in a format that readily permits electronic filing.
6-V	Sidney Powell on Lou Dobbs Tonight on 11/30/20, YouTube (Nov. 30, 2020), available	This exhibit is maintained by counsel and is available upon request. As it is an audio/video,

	at, https://www.youtube.com/watch?v=4uMr-TRZNCw (last visited Jan. 4, 2021).	the exhibit is not in a format that readily permits electronic filing.
14-V	WATCH: Georgia election officials reject Trump call to 'find' more votes, PBS (Jan. 4, 2021), available at, https://www.pbs.org/newshour/politics/watch-live-georgia-secretary-of-states-office-holds-press-conference (last visited Jan. 7, 2021).	This exhibit is maintained by counsel and is available upon request. As it is an audio/video, the exhibit is not in a format that readily permits electronic filing.
20-V	Sidney Powell: Dems will use 'lawfare' to alter election, OAN (Nov. 3, 2020), available at, https://defendingtherepublic.org/?p=1154; https://www.youtube.com/watch?v=Vh5U_6apzvI&feature=emb_logo (last visited Jan. 7, 2021).	This exhibit is maintained by counsel and is available upon request. As it is an audio/video, the exhibit is not in a format that readily permits electronic filing.
22-V	Patrick Byrne Explains Trump Path to Victory, Corsi Nation (Dec. 24, 2020), available at, https://www.stitcher.com/show/corsi-nation-by-jerome-r-corsi-phd/episode/dr-corsi-news-12-24-20-patrick-byrne-explains-trump-path-to-victory-80388895 (last visited Jan. 7, 2021).	This exhibit is maintained by counsel and is available upon request. As it is an audio/video, the exhibit is not in a format that readily permits electronic filing.
25-V	The Rush Limbaugh Show, iHeart Radio (Dec. 29, 2020), available at, https://www.iheart.com/podcast/1119-the-rush-limbaugh-show-57927691/episode/the-rush-limbaugh-show-podcast75675693/ (last visisted Jan. 7, 2021).	This exhibit is maintained by counsel and is available upon request. As it is an audio/video, the exhibit is not in a format that readily permits electronic filing.
26-V	Sidney Powell to Newsmax TV: Our Case Was Prejudged, Newsmax (Dec. 7, 2020), available at, https://defendingtherepublic.org/?p=1166 ; https://www.newsmax.com/newsmax-tv/sidney-powell-kraken-lawsuit-scotus/2020/12/07/id/1000459/ (last visited Jan. 4, 2021).	This exhibit is maintained by counsel and is available upon request. As it is an audio/video, the exhibit is not in a format that readily permits electronic filing.
27-V	Evidence of Fraud: Sidney Powell and Lou Dobbs discuss, Fox Business (Dec. 11, 2020), available at, https://defendingtherepublic.org/?p=1168 ;	

_		T
28-V	Exclusive: Sidney Powell on 2020 Election Lawsuits, Supreme Court Decision, and the Flynn Case, The Epoch Times (Dec. 13, 2020), available at, https://defendingtherepublic.org/? p=1170; https://www.theepochtimes.com/exclusive-sidney-powell-on-election-lawsuits-supreme-court-decision-and-the-flynn-case_3617067.html (last visited Jan. 4, 2021).	This exhibit is maintained by counsel and is available upon request. As it is an audio/video, the exhibit is not in a format that readily permits electronic filing.
29-V	Sidney Powell: Kraken Released in MI; Scotus Next!, The John Fredericks Show (Dec. 14, 2020), available at, https://www.johnfredericks-radio.com/podcast/december-14-2020/ ; https://www.youtube.com/watch?v=qWt1vB-OIZk&list=PL1q2i_zsupwSdYDFTH0pA-X-YNz57E5TV&index=2 (last visited Dec. 29, 2020).	This exhibit is maintained by counsel and is available upon request. As it is an audio/video, the exhibit is not in a format that readily permits electronic filing.
30-V	Sidney Powell to Newsmax: Dominion Designed to 'Rig Elections,' Newsmax (Nov. 17, 2020), available at, https://www.newsmax.com/newsmax-tv/sidney-powell-dominion-voting-systems/2020/11/17/id/997526/ (last visited Dec. 4, 2020).	This exhibit is maintained by counsel and is available upon request. As it is an audio/video, the exhibit is not in a format that readily permits electronic filing.
32-V	Trump Campaign News Conference on Legal Challenges, CSPAN (Nov. 19, 2020), available at, https://www.c-span.org/video/?478246-1/trump-campaign-alleges-voter-fraud-states-plans-lawsuits (last visited Jan. 4, 2021).	This exhibit is maintained by counsel and is available upon request. As it is an audio/video, the exhibit is not in a format that readily permits electronic filing.
33-V	MUST-SEE: Tucker Carlson ABANDONS Trump's election fraud case on air, YouTube (Nov. 19, 2020), available at, https://www.youtube.com/watch?v=BspHzH6 RRxo (last visited Jan. 4, 2021).	This exhibit is maintained by counsel and is available upon request. As it is an audio/video, the exhibit is not in a format that readily permits electronic filing.
36-V	Sidney Powell: It will be BIBLICAL, Newsmax TV (Nov. 21, 2020), available at https://www.youtube.com/embed/Y68pEknYyCM?rel=0&s tart=0 (last visited Jan. 4, 2021).	This exhibit is maintained by counsel and is available upon request. As it is an audio/video, the exhibit is not in a format that readily permits electronic filing.
40-V	BREAKING NEWS: Sidney Powell Tells Lou Dobbs Her Lawsuit in Georgia May Be Filed As Soon As Tomorrow, YouTube (Nov. 24, 2020), available at, https://www.youtube.com/watch?v=KpT2Rz4rTWM (last visited Jan. 4, 2021).	This exhibit is maintained by counsel and is available upon request. As it is an audio/video, the exhibit is not in a format that readily permits electronic filing.

44-V	Sidney Powell, Lin Wood attend 'Stop the Steal' rally in Georgia, YouTube, (Dec. 2, 2020), available at, https://www.youtube.com/watch?v=pq-B5z3QIA (last visited Jan. 4, 2021).	This exhibit is maintained by counsel and is available upon request. As it is an audio/video, the exhibit is not in a format that readily permits electronic filing.
48-V	The Affidavit: Sidney Powell With Lou Dobbs, YouTube (Nov. 16, 2020), available at, https://www.youtube.com/watch?v=n_plsonhp -k (last visited Jan. 4, 2021).	This exhibit is maintained by counsel and is available upon request. As it is an audio/video, the exhibit is not in a format that readily permits electronic filing.
49-V	Sidney Powell Follows Up With Lou Dobbs About Today's Press Briefing, YouTube (Nov. 19, 2020), available at https://www.youtube.com/watch?v=X-53TpxRtxI (last visited Jan. 4, 2021).	This exhibit is maintained by counsel and is available upon request. As it is an audio/video, the exhibit is not in a format that readily permits electronic filing.
51-V	Sean Hannity Radio Show with Louie Gohmert, iHeart Radio (Dec. 23, 2020), available at, https://www.sidneypowells-latest-insight-into-the-fraudulent-2020-election (last visited Jan. 4, 2021).	This exhibit is maintained by counsel and is available upon request. As it is an audio/video, the exhibit is not in a format that readily permits electronic filing.
90-V	Sunday Morning Futures with Maria Bartiromo Sydney Powell ELECTION FRAUD, Fox News (Nov. 9, 2020), available at, https://defendingtherepublic.org/?p=1164; https://www.youtube.com/watch?v=g6swRH3 8oKs&list=PLnpdXA3HSORvJoUVwtdrX2c Mum5d9I8x7&index=28 (last visited Jan. 4, 2021).	This exhibit is maintained by counsel and is available upon request. As it is an audio/video, the exhibit is not in a format that readily permits electronic filing.
93-V	Sidney Powell with Lou Dobbs: Release the Kraken, YouTube (Nov. 14, 2020), available at, https://www.youtube.com/watch?v=SFCXPw1 t170 (last visited Jan. 4, 2021).	This exhibit is maintained by counsel and is available upon request. As it is an audio/video, the exhibit is not in a format that readily permits electronic filing.
94-V	One-on-one with Sidney Powell, KPTM (Nov. 15, 2020), available at, https://app.criticalmention.com/app/#clip/view/3de8b395-d807-4ba7-9855-0af62dc1a005?token=37f52d99-127d-4b48-b8dc-e5e99babfaaa (last visited Jan. 4, 2021).	This exhibit is maintained by counsel and is available upon request. As it is an audio/video, the exhibit is not in a format that readily permits electronic filing.

95-V	Attorney Powell on election legal challenges that remain active in several states, Fox News (Nov. 15, 2020), available at, https://video.foxnews.com/v/6209930642001?playlist_id=3386 https://oioonable.com/v/6209930642001?playlist_id=3386 https://oioonable.com/v/6209930642001 ?playlist_id=3386 <a< th=""><th>This exhibit is maintained by counsel and is available upon request. As it is an audio/video, the exhibit is not in a format that readily permits electronic filing.</th></a<>	This exhibit is maintained by counsel and is available upon request. As it is an audio/video, the exhibit is not in a format that readily permits electronic filing.
96-V	The Rush Limbaugh Show, iHeart Radio (Nov. 16, 2020), available at, https://www.iheart.com/podcast/1119-the-rush-limbaugh-show-podcast-73947607/ (last visited Jan. 4, 2021).	This exhibit is maintained by counsel and is available upon request. As it is an audio/video, the exhibit is not in a format that readily permits electronic filing.
97-V	Sidney Powell to Newsmax TV: Dominion Contracts Warrant Criminal Probe, Newsmax (Dec. 28, 2020), available at, https://www.newsmax.com/newsmax-tv/sidney-powell-georgia-lawsuit-contract/2020/11/28/id/999106/ (last visited Jan. 4, 2021).	This exhibit is maintained by counsel and is available upon request. As it is an audio/video, the exhibit is not in a format that readily permits electronic filing.
98-V	Sidney Powell: "I Have Direct Evidence of Vote Fraud on the Biggest Scale in World History," The John Fredericks Show (Dec. 3, 2020), available at, https://www.johnfredericksradio.com/podcast/december-3-2020/ ; https://www.youtube.com/watch?v=QKzqvtxdwfA (last visited Jan. 3, 2021).	This exhibit is maintained by counsel and is available upon request. As it is an audio/video, the exhibit is not in a format that readily permits electronic filing.
99-V	EXCLUSIVE: Sidney Powell Suspects CIA in RIGGING Elections, Huckabee (Dec. 5, 2020), available at, https://www.youtube.com/watch?v=dNK- LrrzxcE&list=PLp0iqOAbW0sZh0FqV39gW4 NEwn-N0Rp0L (last visited Jan. 4, 2021).	This exhibit is maintained by counsel and is available upon request. As it is an audio/video, the exhibit is not in a format that readily permits electronic filing.
101-V	FlashPoint: Hope Is Not Lost! Featuring Attorney Sidney Powell (The Victory Channel broadcast Dec. 29, 2020), available at https://www.sidneypowell.com/media/flashpoint-hope-is-not-lost-featuring-attorney-sidney-powell (last visited Jan. 3, 2021).	This exhibit is maintained by counsel and is available upon request. As it is an audio/video, the exhibit is not in a format that readily permits electronic filing.
103-V	Sidney Powell – Status of Presidential Election, CATS Roundtable (Jan. 3, 2021), available at, https://www.sidneypowell.com/media/status-of-the-presidential-election (last visited Jan. 3, 2021).	This exhibit is maintained by counsel and is available upon request. As it is an audio/video, the exhibit is not in a format that readily permits electronic filing.

	104-V	Tucker Carlson Tonight, Fox News (Nov. 21, 2020), available at, https://video.foxnews.com/v/6211375866001? playlist_id=5198073478001#sp=show-clips (last visited Jan. 4, 2021).	This exhibit is maintained by counsel and is available upon request. As it is an audio/video, the exhibit is not in a format that readily permits electronic filing.
	105-V	Sidney Powell fires back at Tucker Carlson on Maria Bartiromo morning show, Fox News, YouTube (Nov. 20, 2020), available at, https://www.youtube.com/watch?v=QRptwx0y8sc&t=14s (last visited Jan. 4, 2021).	This exhibit is maintained by counsel and is available upon request. As it is an audio/video, the exhibit is not in a format that readily permits electronic filing.
=	107-V	Global Prayer for US Election Integrity, Adam Schindler (Jan. 3, 2021), available at, https://www.adamschindler.com/prayer/global-prayer-for-us-election-integrity-20/ (last visited Jan. 4, 2021).	This exhibit is maintained by counsel and is available upon request. As it is an audio/video, the exhibit is not in a format that readily permits electronic filing.

Date: January 8, 2021

/s/ Thomas A. Clare, P.C.

Thomas A. Clare, P.C. (D.C. Bar No. 461964) Megan L. Meier (D.C. Bar No. 985553) Dustin A. Pusch (D.C. Bar No. 1015069) 10 Prince Street Alexandria, VA 22314 (202) 628-7400 tom@clarelocke.com megan@clarelocke.com dustin@clarelocke.com

Attorneys for Plaintiffs